FINAL PROJECT – TI 184833

OPERATIONAL RISK ANALYSIS IN PT KREDIBEL TEKNOLOGI INDONESIA BASED ON ISO 31000:2018 WITH FAILURE MODE AND EFFECT ANALYSIS (FMEA) AND BENEFIT COST RATIO

ANNURA RATRI RAMADANTI
NRP. 02411740000069

Supervisor:
Naning Aranti Wessiani, S.T., M.M.
NIP. 197802072003122001

DEPARTMENT OF INDUSTRIAL AND SYSTEM ENGINEERING
Faculty of Industrial Technology and Systems Engineering
Institut Teknologi Sepuluh Nopember
Surabaya
2021

FINAL PROJECT – TI 184833

OPERATIONAL RISK ANALYSIS IN PT KREDIBEL TEKNOLOGI INDONESIA BASED ON ISO 31000:2018 WITH FAILURE MODE AND EFFECT ANALYSIS (FMEA) AND BENEFIT COST RATIO

ANNURA RATRI RAMADANTI
NRP. 02411740000069

Supervisor:
Naning Aranti Wessiani, S.T., M.M.
NIP. 197802072003122001

DEPARTMENT OF INDUSTRIAL AND SYSTEM ENGINEERING
Faculty of Industrial Technology and Systems Engineering
Institut Teknologi Sepuluh Nopember
Surabaya
2021

APPROVAL SHEET

OPERATIONAL RISK ANALYSIS IN PT KREDIBEL TEKNOLOGI INDONESIA BASED ON ISO 31000:2018 WITH FAILURE MODE AND EFFECT ANALYSIS (FMEA) AND BENEFIT COST RATIO

FINAL PROJECT

Proposed to Fulfill the Requirement to Obtain
the Bachelor's Degree of Engineering in
Bachelor Program of Industrial System and Engineering Department
Faculty of Industrial Technology and System Engineering
Institut Teknologi Sepuluh Nopember

Compiled by

ANNURA RATRI RAMADANTI
Student ID 02411740000069

Approved by:
Supervisor

Naning Arafati Yassiani, S.T., M.M.
NIP. 19780207200312001

Surabaya, July 2022

(This page is intentionally left blank)

OPERATIONAL RISK ANALYSIS IN PT KREDIBEL TEKNOLOGI INDONESIA BASED ON ISO 31000:2018 WITH FAILURE MODE AND EFFECT ANALYSIS (FMEA) AND BENEFIT COST RATIO

Name : Annura Ratri Ramadanti
Student ID : 02411740000069
Supervisor : Naning Aranti Wessiani, S.T., M.M.

ABSTRACT

PT Kredibel Teknologi Indonesia or commonly called Kredibel is a big data start up that has an aim to fight online fraud and develop a save online shopping ecosystem. Kredibel only apply risk management for their information security, which based on ISO 27001. Meanwhile, they do not implement risk management in their operational activities or business continuity yet. The operational activities related to the service that they provide, called Fraud Management System (FMS). This can lead to financial loss that even they do not know it occurs. Furthermore, business continuity is important especially for a startup that has a lot of room for human error.

Risk management system that is done to determine the best risk treatment for operational activities of Kredibel that are broken down by using service blueprint. It is applied based on ISO 31000:2018. The risk identification is done by using Failure Mode and Effect Analysis (FMEA) with three risk dimensions, which are severity, occurrence, and detection. The identified risks are differentiated into four level of risk, which are extreme, high, medium, and low. The prioritized risks also defined by using Pareto based on the Risk Priority Number (RPN). Six alternatives of risk treatment scenario are conducted based on the risk categorization. The scenario selection process is done by using benefit cost ratio.

The result of risk identification is 43 risks with proportion of 19% extreme risks, 28% high risks, 30% medium risks, and 23% low risks. All of the risk treatment scenarios are feasible based on benefit cost ratio. Based on incremental benefit cost ratio, the chosen risk treatment scenario is scenario 2 that implements reduce action to all of the risks.

Keywords: Risk Management, Operational Risk, Service Blueprint, ISO 31000:2018, Failure Mode and Effect Analysis, Benefit Cost Ratio

(This page is intentionally left blank)

ACKNOWLEDGEMENT

Praise to Allah SWT, whom by His blessings this research with the title of "Operational Risk Analysis in PT Kredibel Teknologi Indonesia based on ISO 31000:2018 with Failure Mode and Effect Analysis (FMEA) and Benefit Cost Ratio" can be completed in time. This research is done as a requirement to complete Industrial System and Engineering Undergraduate Degree (S1) in Department of Industrial System Engineering of Faculty of Industrial Technology and System Engineering at Institut Teknologi Sepuluh Nopember, Surabaya.

During the process of completing this research, the authors have received many guidance, support, and suggestions from many people. Therefore, in this opportunity, the author would like to express the sincere gratitude to:

1. Naning Aranti Wessiani, S.T., M.M., as the supervisor of this research, for all her guidance, knowledge, suggestion, and support for the author,
2. Fadel Muhamad Iqbal, Muhammad Ihsan, and all stakeholders in PT Kredibel Teknologi Indonesia for the help and suggestion to complete this research,
3. Ir. Lantip Trisunarno, M.T. and Erwin Widodo, M.Eng., Dr.Eng., as the examiner of this research, for all suggestion and correction for the author's work,
4. Nurhadi Siswanto, S.T., M.S.I.E, Ph.D., as the Head of Department of Industrial System and Engineering of ITS as well as all the respectful and distinguished lecturers, for all lesson, knowledge, experience, motivation, and inspiration given to the author during her study,
5. Author's beloved family, Ibu Endah, Bapak Budi, Mbak Pipit, Mas Rando, and Feyrin for all the endless love, prayer, and support for the author,
6. All of author's companions, especially Isfan, Aafini, Adisvia, Alam, Andina, Gischa, Hakim, Jasmine, and Phoebe for the motivation, inspiration, and moral support for the author,
7. Author's colleagues at PSMI Laboratory, for the endless support and insights for the author during her study.

Lastly, for everyone who indirectly contributed to the completion of this research, may Allah SWT bless us all with His grace. In the completion of this research, author is aware that there are still rooms for improvement in this research. Hence, author expects critics and suggestions from the readers so that this research can be developed and become more beneficial for us all. May this research be useful for all readers.

Surabaya, July 2021

Author

TABLE OF CONTENTS

LIST OF FIGURES

(This page is intentionally left blank)

LIST OF TABLES

CHAPTER 1
INTRODUCTION

In this chapter, there will be explanation about the basic things related to the research done by the author, that consist of research background, problem formulation, objectives, benefits, scopes, and the report writing systematics.

1.1 Background

Big data company is a company which offers products that requires to taking very large sets of complex data from multiple population and analyzing it to find patterns, trends, problems to gain actionable insights (Schroer, 2019). Big data companies are emerging nowadays. The global annual growth rate of big data technologies and services is predicted to increase about 36% between 2014 and 2019, with the global income for big data and business analytics may increase more than 60% (Hariri, et al., 2019). It is because the companies that using big data are able to provides solution effectively and people needs these new ways of problem-solving. The benefits that those companies can give to their customers in term of problem-solving are speed and efficiency (SAS, 2021). Previously, a business would have gathered information and make analytics so it can be used for future decision. Today, business can make insight from the information quickly, even it can be used for immediate decision. In ASEAN, Indonesia has the highest number of companies that already used big data (JawaPos.com, 2019). Usually, the implementation of big data is followed by other advance technology, such as artificial intelligence (Novianty, 2020). In Indonesia, 65% of local business community already implemented big data, artificial intelligence, and IoT. This technology is applied because it may decrease the risk of wrong decision making and operational cost up to 25% (JawaPos.com, 2019).

Online fraud is fraud that is committed through the internet. Online fraud can be divided into two, which are financial fraud and identity theft or fake identity (Lewis & Clark, 2010). Online fraud can be in many forms. One of them is online shopping fraud. This from of online fraud rely on the anonymity of the internet (Action Fraud, n.d.). Online shopping fraud commonly involve buyers not receiving

the goods, sellers not receiving payment, irrelevant information about a product or the terms of sale, and others. As the increasing of internet shopping popularity, the number of complaints about online shopping transaction is increasing. Globally, online shopping fraud loss reaches $57.8 billion in 2017, increased for about 5.5% from 2016 (Security Magazine, 2017). In Southeast Asia, there are top 5 e-commerce markets, which are Philippines, Malaysia, Thailand, Singapore, and Indonesia. In 2018, Indonesia has the highest losses from online shopping fraud for about 3.2% of the total revenue and have probability of twelve times more likely to be fraudulent than global average (Yeo, 2019).

PT Kredibel Teknologi Indonesia or commonly called Kredibel is one of a big data start up in Indonesia. It is a B2B and B2C company that has an aim to fight online fraud and develop a save online shopping ecosystem. Its service is based on complains and reports from user that ever had a transaction with the fraudsters. This company already recorded hundred thousands of fraud case and thousands of fraudster's bank accounts with total financial loss of more than Rp250.000.000 (Kredibel, 2016). In Indonesia, this kind of business is still rare. The only competitor of their B2C business is a website that is managed by the government, specifically Kementerian Komunikasi dan Informasi, called CekRekening.id. Meanwhile, for their B2B business, which is their main profit source, does not have any competitor.

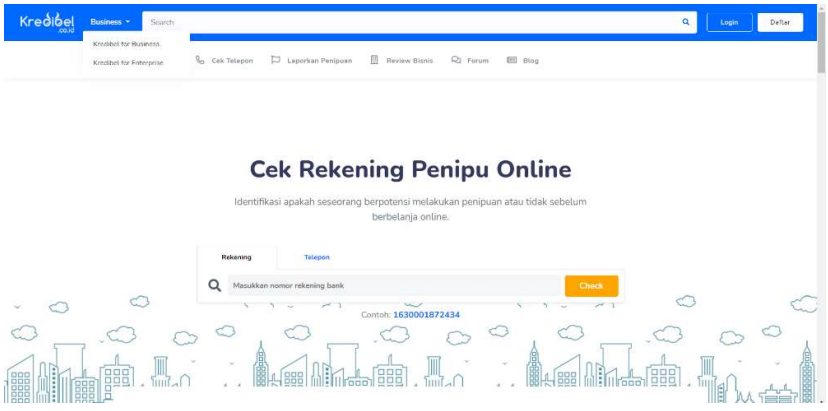

Figure 1.1 Kredibel Home Page

(Source: PT Kredibel Teknologi Indonesia, 2016)

Risk management is a process of identifying, assessing, and controlling potential threats or risks to an organization's capital and earnings (Rouse, 2020).

Risk management is needed in order to face the unexpected harmful events so that the company are able to minimize the risks and extra cost that may occur because of the risk itself. By implementing risk management, the company are able to conduct plans or procedures for all the potential harmful events before they occur. With the presence of risk management, the company can protect their business decision and help them to reach their goals. Risk management is important for any kinds of companies because each company have their own risks that came from the uncertainty of internal and external environment. Without risk management, a company may fall on heavy loses that they even did not know it occurred (Wilson, 2020).

As a company that provides accurate data analytics, PT Kredibel Teknologi Indonesia have to ensure their data security. They already implemented ISO 27001 standard. This standard describes how a company should organize its information security (Kosutic, 2014). Information security is a part of risk management and have to align with the standard that is used for risk management. ISO 27001 itself already mentioned that the information security management procedures in it is aligned with ISO 31000, as the common ISO standard that is used for risk management. However, a company could use other risk management standard as long as it suitable with ISO 27001. Here is a picture that explain the relationship between information security and risk management.

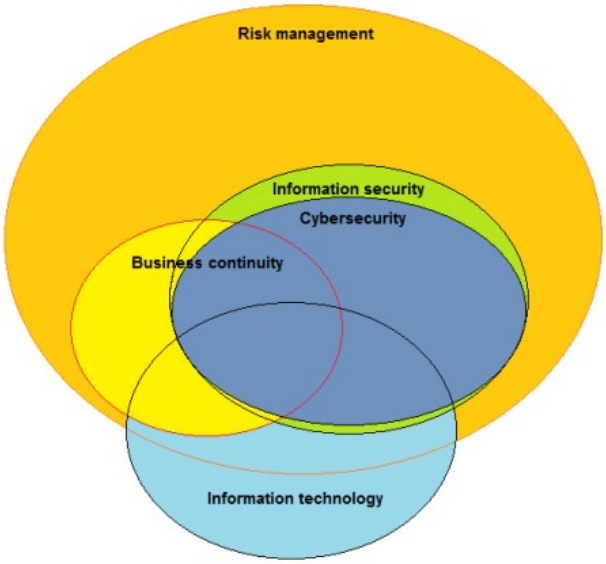

Figure 1.2 Relationship between Information Security and Risk Management (Source: advisera.com, 2014)

The risk management that already implemented in Kredibel is only in term of data or information security as the requirement of ISO 27001. For the business itself or commonly called business continuity, Kredibel is not implementing any standard for the risk management yet. In short, Kredibel does not have any special department or function that focus on risk management of business continuity and has not done any risk management for their business activities, that starts from risk identification until risk treatment.

ISO 31000 is an international standard of risk management that first published in 2009, with the updated version in 2018. This standard can be used broadly across any industries and business types to provide the best practice structure and guidance of risk management (Peterson, 2019). The usage of ISO standard may give competitive advantage to the company because it is internationally well known and a symbol for quality standard. Furthermore, ISO 31000 is chosen rather than other ISO standard in term of management system, such as ISO 9001 and ISO 14001 because in term of risk management ISO 31000 is more superior in risk assessment process. The risk assessment process in ISO 31000 is divided into risk identification, analysis, evaluation, and treatment. While ISO 9001 and ISO 14001 only elaborate the definition of risk as the effect of uncertainty, without explaining the process of risk assessment (Confirmative, 2021).

In implementing risk management, other approach will be used to conduct risk identification. Failure Modes and Effects Analysis (FMEA) is used to identify all possible failures in a design or manufacturing process of product or service (ASQ, 2021). This approach is able to define the severity, occurrence, and detection of each possible failures. Then, the level of each of possible failures can be determined. FMEA is selected rather than Fault Tree Analysis (FTA) because FMEA uses bottom-up approach and focus to identify all possible internal failures modes separately without considering any relationship between multiple failures which is more suitable for start-up that still has a lot of room for human error (Infraspeak, n.d.). FMEA creates an isolated system and does not consider the external factors. While FTA use top-down approach and only focus on the relationship between multiple failures that leads to the “top events”. It also neglects

the partial failures so that not all the possible failures can be identified, which is not in line with the main purpose of this research.

In Kredibel, there are two main departments that consists of several functions for each department. These two departments are Business Department and Product and Engineering Department. Product and Engineering Department is mainly about data and data security which already implemented risk management as the requirement of ISO 27001 that already mentioned before. As already mentioned before, the risk management in this research will be applied to business continuity. Business continuity risk management is related to all risks that can affect the company's operations (Kenton, 2020). Therefore, in this research, the author will focus on operational activities that are directly related to the customer under Business Department. Thus, the risk management will be applied for the main service, which called Fraud Management System that is offered by PT Kredibel Teknologi Indonesia. Here is the company's organizational structure.

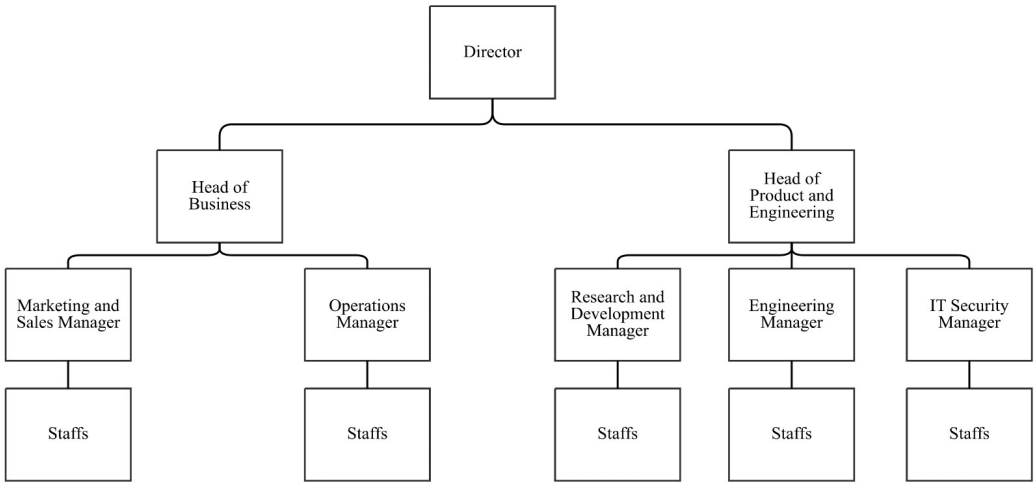

Figure 1.3 Kredibel Organizational Structure
(Source: PT Kredibel Teknologi Indonesia, 2016)

Based on the explanation above, this research will contain risk management in operational activities of PT Kredibel Teknologi Indonesia based on ISO 31000. ISO 31000 is selected because it adaptable and applicable to all companies, in term of type, size, activities, and covers all types of risk (Risk Decisions, 2020). Furthermore, it also has accessible structure and easy to implement because it covers the whole process of risk management, which are the principles, framework,

and process (Risk Decisions, 2020). Risk definition and risk analysis phase will be done by FMEA approach to make sure that there is no potential failure missed and the risk treatment for each potential failure will be more accurate. Benefit Cost Analysis also used the reference for the company to choose the best risk treatment alternative scenario that is defined in the previous phase. The cost of risk treatment alternative scenario will be calculated, and it will be compared with the benefit that obtained from the risk treatment alternative scenario. The scenario that is chosen is the scenario that the benefit is higher than the cost.

This research is expected to be able to help PT Kredibel Teknologi Indonesia in defining risk profile and the best risk treatment alternative scenario in order to improve their business activities. Since there are still a few similar companies in Indonesia, the improvement of this company's business activities hopefully can reduce fraud cases in Indonesia especially in online shopping environment.

1.2 Problem Formulation

Based on the background that already explained above, the formulated problem that will be the focus of this research is about how to determine the best risk treatment alternative scenario for operational activities of PT Kredibel Teknologi Indonesia based on the risk profile and benefit cost ratio.

1.3 Research Objectives

Here are the objectives of this research.

1. Define potential failures or risks for operational activities of PT Kredibel Teknologi Indonesia.
2. Define the risk profile of operational activities in PT Kredibel Teknologi Indonesia using FMEA approach.
3. Give risk treatment recommendation for every risk based on the profile for operational activities of PT Kredibel Teknologi Indonesia.
4. Conduct benefit cost ratio to choose the best risk treatment alternative scenario in operational activities of PT Kredibel Teknologi Indonesia.

1.4 Research Benefits

Here are the benefits that can be obtained by doing this research towards PT Kredibel Teknologi Indonesia.

1. PT Kredibel Teknologi Indonesia could know the potential failures or risks that might happen in operational activities.
2. PT Kredibel Teknologi Indonesia could know which risks that being prioritized in operational activities based on the risk profile.
3. As a reference for PT Kredibel Teknologi Indonesia about the right risk treatment scenario for every potential risk in operational activities.
4. PT Kredibel Teknologi Indonesia could know the benefit cost analysis for the recommended risk treatment alternative scenario in operational activities.

1.5 Research Scopes

The scopes of this research are differentiated into two types, which are limitations and assumptions.

1.5.1 Limitations

Here are the limitations of this research.

1. The observed object consists of operational activities, which is related to their service offered.
2. The risks that are related with data or information security are not included in this research.
3. The risks that are identified only risks that give negative impact to the company.
4. The alternative treatments assigned are maximum two treatments per risk.
5. The benefit cost ratio only considers the direct financial impact.
6. The company risk treatment alternative scenario plan is conducted only for 2021-2022.
7. The main data source is the head of business that fully understand about Fraud Management System.
8. Data collection is done completely online.

1.5.2 Assumptions

Here are the assumptions of this research.

1. There is no change in regulation and condition that influence the company during this research.
2. The data collected is valid because it is from the experts that understand about the whole activities under Business Department, especially about their operational activities.

1.6 Report Writing Systematics

The report of this research consists of six chapters. Here are the report writing systematics that consist of the brief explanation for each chapter.

CHAPTER 1 INTRODUCTION

In this chapter, there will be explanation about the basic things related to the research done by the author, that consist of research background, problem formulation, research objectives, research benefits, research scopes, and the report writing systematics.

CHAPTER 2 LITERATURE REVIEW

In this chapter, there will be explanation about methods that are used in this research and also supporting theories that are used as the basic of this research, especially in chapter data collection and processing.

CHAPTER 3 RESEARCH METHODOLOGY

In this chapter, there will be flowchart and explanation of the flowchart about the step by step of methodology that is used in this research. The methodology contains the flow of the research starts from data collection, data processing, data analysis and interpretation, and drawing conclusion and suggestion.

CHAPTER 4 DATA COLLECTION AND PROCESSING

In this chapter, there will be explanation about result of data collection and the process of the research based on the objectives and methodology that already mentioned in the previous chapter.

CHAPTER 5 DATA ANALYSIS AND INTERPRETATION

In this chapter, there will be explanation about the analysis and interpretation of the data processing result from chapter 4. The context of this

chapter depends on the objectives that already stated in the beginning of this research.

CHAPTER 6 CONCLUSION AND SUGGESTION

In this chapter, there will be conclusion regarding this research based on the objectives that already determined by the author in the beginning of this research and also suggestion from the author to improve the further research development.

(This page is intentionally left blank)

CHAPTER 2
LITERATURE REVIEW

In this chapter, there will be explanation about methods that are used in this research and also supporting theories that are used as the basic of this research, especially in chapter data collection and processing.

2.1 Risk

Risk is the potential of a situation or event to impact on the achievement of specific objectives. Risk can be perceived either positively or negatively (Association for Project Management, 2020). According to Hampton (2009), risk is the likelihood that actual results will not match expected results. Risk has two factors, which are effect of event on the project outcome and probability of occurrence of the factor or event (Merna, 2008). According to ISO 31000, risk is the effect of uncertainty on objectives and an effect is a positive or negative deviation from what is expected (Praxiom, 2018).

2.1.1 Types of Risks

Here are the main types of risks that a company may face (Blackman, 2014).

1. Strategic Risk

   This kind of risk can make the company's strategy become less effective in reaching its goals. It may occur when a company gets stuck in selling their products because it does not accompany by a good plan. It could be because of technological changes, a new competitor that enter the market, the shifting of customer demand, the increasing of raw materials costs, or others.

2. Compliance Risk

   This kind of risk happened when there are additional regulations appeared. The laws that might change all the time and the business that keep expands will make a company have to comply with new rules that are not being applied before. The extreme case of compliance risk may become a strategic risk if it has impact to the business' future. It could

be because of regulation in finance, healthcare, manufacturing, or technological issues.

3. Operational Risk

   This kind of risk refers to failures that are related to company's core operation activities. The risk can be a technical failure that caused by internal factors, such as people, processes, or machines, that can disrupt company's ability to do their operational process. Besides internal factors, operational risk can also happen due to external factors, such as natural disaster, power shutdown, server problem, or others.

4. Financial Risk

   Most of the risk will have financial impact either directly or indirectly. This kind of risk specifically refers to the money flowing in and out of the business and the possibility of a sudden financial loss. For example, it is related to the ability of a company afford their payment or when some customers are not able to fulfill their payment on time. This risk commonly increases when a company expand the business globally.

5. Reputational Risk

   Reputation is important for every companies. This risk that can damage the reputation may give impact to the loss of revenue, demoralized employees, and the loss of suppliers, partners, and investor. It could be due to the negative image of employees, bad review of the products or services, and others.

2.1.2 Cause of Risk

Basically, there are three main causes of risk. Here is the explanation of each cause (Corporate Finance Institute, 2015).

1. Natural Causes

   This kind of causes include disaster, such as flood, earthquake, typhoon, and many others. Basically, it cannot be controlled by human. However, it can result high number of losses and the prevention action is quite difficult.

2. Human Causes

   This kind of causes refer to the employees' lack of attention at work, mismanagement, and others. It is usually the main cause of risks that are related with core operational activities.

3. Economic Causes

   This kind of causes related to the chance of financial loss due to the market or competition change, raw material pricing, labor cost, and others. The loss is happened because it has direct impact to the earning of the business.

2.2 Risk Management

Risk management is the process of identifying, assessing, and controlling threats to an organization's capital and earnings (Cole, 2020). Every business has to apply risk management because there must be unexpected risks that have to faced and these risks will lead to harmful events that cost the company or even permanently close the company. Risks have either positive or negative impact to the company. Thus, risk management is focused to minimizing the impact of negative risk and maximizing the impact of positive risk, mostly in term of cost. Effective risk management means attempting to control, as much as possible, future outcomes by acting proactively rather than reactively (Corporate Finance Institute, 2015). Thus, risk management is effective if both possibility of a risk occurring, and risk potential impact are reduced. Before that, a good risk management have to measure the uncertainty and the impact of the risk. Then, a company have to choose between accepting or rejecting risks, that will determine how much the impact to the business. Acceptance or rejection of risks depends on the tolerance level or risk appetite that has already defined by the company. To implement risk management, the first step is to define commitment or standard that used. Then, the company have to design the framework. It means, they have to aware the whole actions, procedures, and processes that happen within the scope of the risk management. After that, the company implements the framework that already defined before. The last is monitor the outcome and improve the outcomes, if necessary, based on the review. Here is the summary of risk management life cycle.

Figure 2.1 Risk Management Life Cycle

(Source: cio-wiki.org, 2020)

2.2.1 Risk Management Purpose

As explained above, the common purpose of risk management is to minimize the impact of negative risk so that the company does not have to spend a lot of money if the risk happened. Other than that, here are the key purposes of risk management (Veyrat, 2016).

1. Risk management is able to align the company's risk appetite with the strategy formulated. The strategies are analyzed and defined into some objectives. Then, the risks will be managed by considering these objectives and also the risk appetite.
2. Risk management provides accurate selection of alternative risk response or treatment, regarding how to avoid, reduce, share, and accept risks. It allows company to strengthen the decision in response to risks.
3. Risk management are able to identify the potential failures and the resulting events. Thus, the surprises and associated loss can be reduced.
4. Risk management allows company to define all the potential events. Therefore, the company is able to take the advantage of the positive risks proactively.
5. Risk management can conduct an effective assessment of the capital needs with adequate information. It may help company to optimize the usage and allocation of their capital.

2.2.2 Risk Management Standard

Risk management standards are able to give guideline regarding framework, processes, and practice. It commonly developed by several worldwide organizations. These standards are used to help a company to do risk management systematically and effectively. Different standards provide different benefits to be used in different situations based on the requirement of each company or organization. Here are risk management standards that are commonly used by a company (CIO Wiki, 2020).

1. ISO 31000:2018 – Risk Management Principles and Guidelines developed by International Standards Organization in 2009 and updated in 2018.
2. IRM (The Institute Risk Management) – Risk Management Standard developed by The Association of Insurance and Risk Manager (AIRMIC) and ALARM the National Forum for Risk Management in public sector in 2002.
3. IEC 31010:2009 – Risk management and Risk Assessment Techniques developed by The International Electrotechnical Commission in 2009.
4. COSO 2004 – Enterprise Risk Management and Integrated Framework developed by The Committee of Sponsoring Organizations in 2004.
5. OCEG "Red Book" 2.0:2009 – A Governance Risk and Compliance Capability Model developed by The Open Compliance and Ethics Group in 2009.

2.3 Business Continuity

Business continuity or Business Continuity Planning (BCP) refers to a part of risk management that involves defining risks that can affect the company's operational activities (Kenton, 2020). This process allows company to determine how those risks will affect the operations and define how to mitigate those risks. It will ensure if a company or organization will have the capability to operate its critical business functions even though there are many risks or emergency events that might happen (Long, 2017). Those events include any event that occurs a disruption of the company's business operation, both events that will stop the

operation completely and events that have potential to adversely impact services or functions. Basically, business continuity planning establishes risk management processes and procedures that has a purpose to prevent interruptions in any services and reestablish the function of the organization as quickly and smoothly as possible. Here are three key components of a business continuity plan (Sullivan, 2020).

1. Resilience

   Resilience can be increased by an organization by designing critical functions and infrastructures. Resilience is important because it can help organizations to maintain essential services on location and off site without interruption.

2. Recovery

   Rapid recovery to restore business function after an emergency event is important. By setting recovery objectives for different systems, networks, or applications can help prioritize which elements must be recovered first.

3. Contingency

   Contingency plan consists of procedures that distributes responsibilities within the organization. These procedures are important in ensuring the reestablishment of the organization's function when the risk or emergency event happen.

2.4 Service Blueprint

Service blueprint is a diagram that explains and visualizes the relationship between each component of a service (Gibbons, 2017). This blueprint is a mapping tool that is used to understand the process in a service in order to discover things that may go wrong (Pugh, 2021). It is closely related to a specific customer journey. A service blueprint is able to elaborate a complex and multi-layered process inside a service. It offers a flexible look for both organization and customer's perspective. A service blueprint provides cross-functional relationship between any roles that performed by human beings or other types of entities, such as organizations, departments, artificial intelligences, machines, or others (Service Design Tools, n.d.).

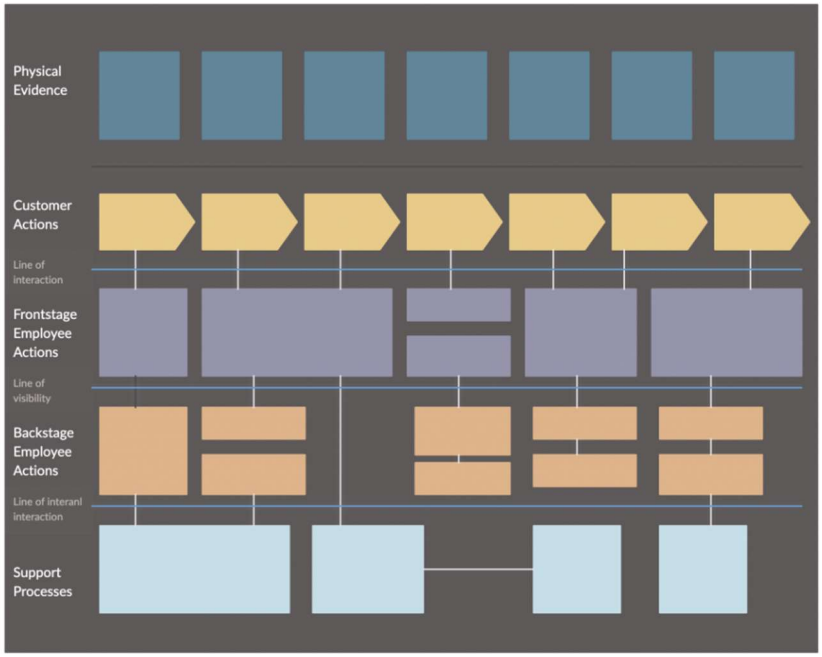

Figure 2.2 Service Blueprint

(Source: Creately, 2020)

Service blueprints may have different forms and shapes. However, every service blueprint consists of these key elements (Creately, 2020).

1. Physical Evidence

   This element refers to anything tangible that is used as the main channel to interact between customers and employees. It is usually the last element that is added to the diagram.

2. Customer Action

   This element refers to any step, choices, activities, and interactions that customers do during the service experience. These actions are displayed chronologically and usually put first to the diagram.

3. Frontstage Action

   This element refers to any actions occurred that directly in view of the customers. These actions can be an interaction from human or from technology. The customer usually experiences it once they have taken an action.

4. Backstage Action

   This element refers to any actions, preparations, or responsibilities taken by the employees to make the service possible, but the customers are unable to see it.

5. Support Process

   This element refers to any additional activities that are carried out by individuals or units within the company to support contact employees deliver the service. These actions are also not visible to the customers.

6. Lines

   These lines are used to separate each category and clarifying the interaction between each element. There are three lines. The first line, which is line of interaction, represents direct interaction between customer and the organization. The second line, which is line of visibility, explains that all components above this line are visible to the customer while the ones below it is invisible. The last line, which is line of internal interaction, separates the employee activities from other service support.

7. Arrows

   The arrows represent relationship or dependencies between actions. A single arrow indicates a one-way exchange while a double arrow indicates the need for agreement from both parties. These arrows help employees to understand their role and any possible customer dissatisfaction during service.

2.5 ISO 31000:2018

ISO 31000 is a risk management standard that first published in 2009 and developed by the International Standard Organization (ISO). It is an international standard that has wide implementation and accepted by many countries with various types and size of organization. ISO 31000 is not an instruction to cope with certain regulation. It is a guideline to cope with uncertainty of business condition and how to deal with them (Enterprise Risk Management Academy, 2010). The benefit of this standard is the threats can be defined more proactive and make the opportunities

more profitable (Mallens & Kruf, 2013). It consists of three components, which are principles, framework, and process of managing risks. Therefore, it is much more comprehensive, systematic, and universal than other risk management standards. ISO 31000 standard summary can be seen in the figure below.

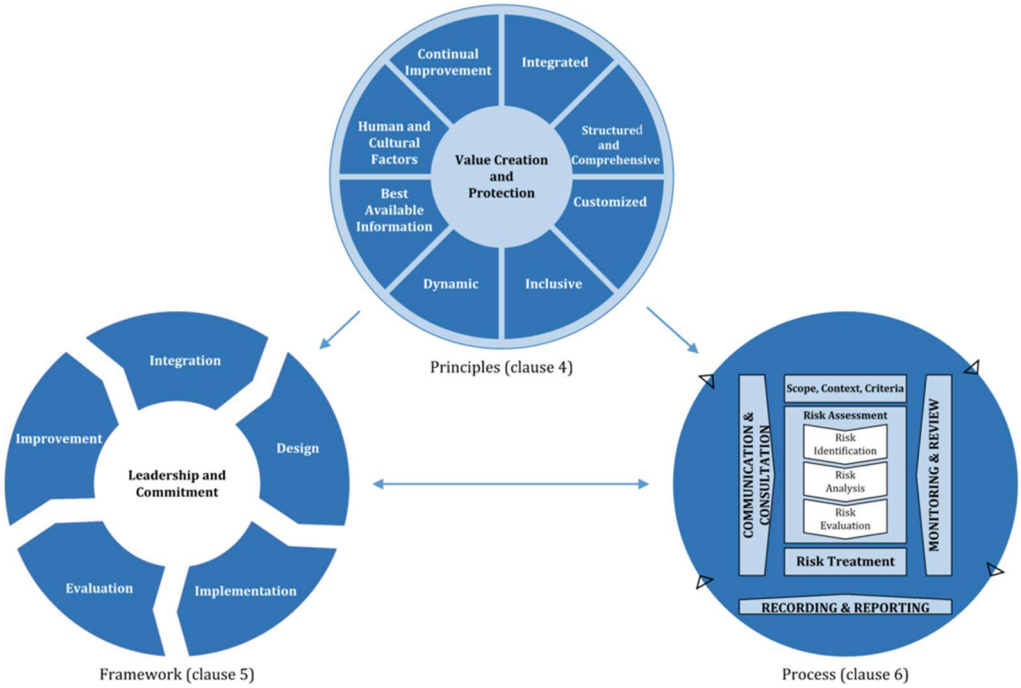

Figure 2.3 Principles, Framework, and Process

(Source: iso.org, 2018)

2.5.1 Principles

In risk management implementation based on ISO 31000, there are eight principles or core ideas that have to followed. These principles are the soul of the risk management structure (Mallens & Kruf, 2013). It describes the most important factors for an effective and efficient risk management framework according to ISO 31000 (Peterson, 2019). Here is the explanation of each point of ISO 31000:2018 principles (ISO, 2018).

1. Integrated

   Risk management is a part of organization that must be integrated to all organizational activities.

2. Structured and comprehensive

   The approach that is structured and comprehensive can leads to consistent and comparable results.

3. Customized

   The process and framework should be customized and match with organization's context and goals.

4. Inclusive

   All stakeholders have to highly participate in risk management implementation by giving their knowledge, views, and perception.

5. Dynamic

   Risk management must be dynamic, as an organization's external and internal context changes. Organization must be able to anticipate, detect, acknowledge, and respond to those changes and events.

6. Best available information

   Risk management uses historical and current information, also future expectation as the inputs. The limitations and uncertainties are associated with these information and expectations. The information should be timely and available to all relevant stakeholders.

7. Human and cultural factors

   Risk management must consider human and cultural factors at all levels and stages.

8. Continual improvement

   Risk management is continuously improved through experience and learning.

2.5.2 Framework

Risk management framework has an aim to help organization in integrating risk management into significant activities and functions. This framework consists of information about how to achieve every point in principles (Peterson, 2019). It describes the function of risk management based on ISO 31000:2018 (Mallens & Kruf, 2013). The effectiveness of risk management will depend on the integration of every component in the framework. Here is the explanation of each component of risk management framework (ISO, 2018).

1. Leadership and commitment

   Top management and oversight bodies should ensure that risk management is integrated with all organizational activities and also the leadership and commitment should be implemented by various activities that mentioned in the guidelines.

2. Integration

   The effectiveness of risk management will depend on how well it is integrated with organizational context. Integrating risk management with organization is a dynamic and iterative process that should be customized depend on the organization's needs and culture. Risk management should be a part of organizational purpose, governance, leadership and commitment, strategy, objectives, and operations.

3. Design

   This component with the next three components also known as a model of continuous quality improvement. These four stages begin with planning and ending with improvement, with the common goal of improving risk management framework (Peterson, 2019). Design stage refers to set some objectives and conduct a plan on how to achieve them.

4. Implementation

   Implementation stage refers to execute the plan. However, there is still possibility that planning still happening here. This stage requires engagement and awareness of stakeholders.

5. Evaluation

   Evaluation stage refers to compare the actual outcome with the desired outcome. Gap analysis will be conducted based on the review of the outcomes by using analytical method and feedback from the process.

6. Improvement

   Improvement stage refers to how the organization adapt to the risk management and continuous improvement since risk management is a cyclic and continuous approach that always have room for improvement. The organization have to make sure that all the employees understand and are able to take ownership of the risk management

process so that they will have motivation and responsible to improve the whole process of risk management.

2.5.3 Process

The risk management process explains how to apply policies, procedures, and practices to communicating and consulting activities. It also explains about assessing, treating, monitoring, reviewing, recording, and reporting risk. The process of risk management must align with the structure, operations, and processes of the organization so it is customizable depends on the context of internal and external condition of the organization. Here is the explanation of each component of risk management process (ISO, 2018).

1. Communication and consultation

   Communication and consultation are a continual and iterative dialogue that has aims to make sure all stakeholders understand risk and the reason of all decision and action that taken by the organization. Besides, this dialogue also helps to understand stakeholders' interests and concern regarding risks, form, likelihood, impact, acceptance, treatment, and others. Communication has purpose to give awareness and ownership about the risk, while consultation has purpose to gain feedback and sufficient information that used for organizational decision-making. It has to be done within all steps of the risk management process and accompanied by expertise from different areas to provide sufficient knowledge.

2. Scope, context, and criteria

   The purpose of this step is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment. The scope of risk management is important because it is related with the organizational objectives that is being considered. The scope that is applied can be strategic, operational, program, project, or other activities. In defining scope, an organization needs to consider objectives and decision that need to be made, expected outcomes, time, location, inclusion and exclusion, appropriate tools and techniques,

required resources, and relationship with other projects, processes, and activities. Context refers to the internal and external environment of the risk management implementation. It should be defined in order to achieve organization objectives accurately. It also can help the organization to define the risks better because the context related with the source of risk. Criteria refers to the type of risk that may or may not take. It related to the organization's values, objectives, and resources, and also aligned with the risk management framework. In defining criteria, an organization needs to consider the uncertainty that may occurred, the definition and measurement of consequences and likelihood, time-related factors, level of risks that is determined, combination and sequences of risks that will be taken, measurement method, and organization capacity.

3. Risk assessment

   Risk assessment is a process that consists of three separate processes, which are risk identification, risk analysis, and risk evaluation. It has to done systematically, iteratively, and collaboratively, equipped with sufficient information.

   Risk identification is a process that allows organization to find, recognize, and describe the risks that could prevent them in achieving their objectives. Factors that should be considered in identifying risk are negative or positive consequences, vulnerabilities and capabilities, context changes, and other supporting details.

   Risk analysis is a process that allows organization to understand the nature, sources, causes, likelihood, and consequences of risks in order to determine the level of risks.

   Risk evaluation is a process that allows organization to compare risk analysis result with risk criteria to determine whether each risk is acceptable or not and what additional action that is required.

4. Risk treatment

   Risk treatment is a process to select and implement additional action to the unacceptable risks. When selecting risk treatment options, the

organization should consider the values, perceptions, and the possibility of how the stakeholders will involve to the risk treatment implementation, also how to communicate and consult with them in the most appropriate way. In this process, a risk treatment plan is conducted to clearly specify how the selected treatment options will be implemented.

5. Monitoring and review

   Monitoring refers to continually check and supervise every steps of risk management. It is done to measure if expected result of each step is being achieved and the deviations if it is not achieved yet. Review refers to an activity to determine if every step is still suitable, effective, and appropriate to implement. It also defines the progress of the risk management and how well the risk management policy is being followed.

6. Recording and reporting

   This step refers to documenting and reporting risk management process and its outcomes. It has aims to give awareness and information about risk management activities and its outcomes across the organization in order to provide for decision-making. Besides, this information could improve the future risk management activities. It also allows interaction between stakeholders that has responsibility and accountability within the risk management activities.

2.6 Failure Mode and Effects Analysis (FMEA)

Failure Mode and Effects Analysis (FMEA) is an approach for defining potential failures or risks early before it happens. It is done to determine the effects and prepare actions to overcome the failures (DSI International, 2017). This approach is easy implemented and provides a well-documented record of the risk profile as well as the corrective actions. The record will be used as historical information about the product design or process and will be continuously improved. However, FMEA depends on subjective assessment, so it needs an expert or a well experienced employee in conducting the analysis. There are three main types of

FMEA. Here is the explanation of each FMEA type (Pereira, 2019). The first type is System FMEA, that is used to analyze complete systems and/or sub-systems. The second type is Design FMEA, that is used to analyze a product design. The last type is Process FMEA, that is used to analyze manufacturing and/or assembly process. Commonly, FMEA consists of 10 steps but can be customized depends on the organization's needs. Here is the explanation of each FMEA step (Schenkelberg, 2014).

1. Review the process or product.

   The first step is to define the subject of the FMEA regarding the functions of components in every process or part of product. The purpose of this step is to make sure all the related stakeholders have the same perception about the product or process that is being observed. It is better to use another approach that is able to determine the detail of the FMEA object, for example flowchart.

2. Brainstorm potential failure modes.

   This step is a process to predict what can go wrong in each component of the process or product. There might be more than one potential failures in each component. Historical data from existing document or report will be highly beneficial in this step. It could be an iterative process to make sure that there is no potential failure that is missed.

3. List potential effects of each failure mode.

   This step refers to define what might occur if the failure mode happens. It also possible to have more than one effect for each failure mode. The effects need to be determined in order to develop a proper solution to overcome the failure modes.

4. Assign a severity ranking for each effect.

   In this step, there will be a score for each failure modes in term of severity or consequence. It means how serious the impact of a failure mode that occur. Severity ranking is driven by the effect. The common range of the score is 1 for the lowest and 10 for the highest. However, the score and its criteria can be customized by the organization as long

as all the stakeholders aware and agree to the scoring system. Here is the basic and common severity scoring system for process that is provided by FMEA approach.

Table 2.1 Severity Scoring System for Process FMEA

Effect	**Criteria: Severity of Effect on Process**	**Rank**
Failure to meet safety and/or regulatory requirements	May endanger operator (machine or assembly) without warning.	10
	May endanger operator (machine or assembly) with warning	9
Major disruption	100% of product may have to be scrapped. Line shutdown or stop ship.	8
Significant disruption	A portion of the production run may have to be scrapped. Deviation from primary process including decreased line speed or added manpower.	7
Moderate disruption	100% of production run may have to be reworked offline and accepted.	6
	A portion of the production line may have to be reworked offline and accepted.	5
Moderate disruption	100% of production run may have to be reworked in-station before it is processed.	4
	A portion of the production run may have to be reworked in-station before it is processed.	3
Minor disruption	Slight inconvenience to process, operation, or operator.	2
No effect	No discernible effect.	1

(Source: Carlson, 2018)

5. Assign an occurrence ranking for each failure mode.

In this step, there will be a score for each failure mode in term of occurrence or frequency. It means how often the cause of the failure is likely to occur. Occurrence ranking is driven by the cause. The common range of the score is 1 for the lowest and 10 for the highest. However, the score and its criteria can be customized by the organization as long as all the stakeholders aware and agree to the scoring system. Here is the basic and common occurrence scoring system for process that is provided by FMEA approach.

Table 2.2 Occurrence Scoring System for Process FMEA

Occurrence of Failure	**Criteria: Occurrence of Causes**	**Rank**
Very high	≥ 1 in 10	10
High	1 in 20	9
	1 in 50	8
	1 in 100	7
Moderate	1 in 500	6
	1 in 2000	5
	1 in 10,000	4
Low	1 in 100,000	3
	1 in 1,000,000	2
Very Low	Failure is eliminated through preventive control	1

(Source: Carlson, 2018)

6. Assign a detection ranking for each failure mode and/or effect.

In this step, there will be a score for each failure mode in term of detection. It means if the effect of a failure is detectable of not. Detection ranking is driven by the current process control. The common range of the score is 1 for the lowest and 10 for the highest. However, the score and its criteria can be customized by the organization as long as all the stakeholders aware and agree to the scoring system. Here is the basic

and common detection scoring system for process that is provided by FMEA approach.

Table 2.3 Detection Scoring System for Process FMEA

Opportunity for Detection	**Likelihood of Detection**	**Rank**
No detection opportunity	Almost impossible	10
Not likely to detect at any stage	Very remote	9
Problem detection post processing	Remote	8
Problem detection at source	Very low	7
Problem detection post processing	Low	6
Problem detection at source	Moderate	5
Problem detection post processing	Moderately high	4
Problem detection at source	High	3
Error detection and/or problem prevention	Very high	2
Detection not applicable, error prevention	Almost certain	1

(Source: Carlson, 2019)

7. Calculate the risk priority number for each effect.
   Risk Priority Number (RPN) is calculated to define the risk priority. Each failure mode RPN will be compared with other failure mode RPN. The highest the RPN, the highest the priority of the failure mode. Here is the formula of RPN.

$$RPN = Severity\ x\ Likelihood\ x\ Detection \quad (2\text{-}1)$$

8. Prioritize the failure modes for action.
   In this step, the failure modes with high RPN will be focused to work on. The 80/20 rule also can be applied in prioritizing failure modes. This means that 80 percent of the total RPN for the FMEA comes from 20 percent of the potential failures and effects.

9. Take action to eliminate or reduce the high-risk failure modes.

   This step refers to implementing the action plan that consist of steps of solution that needed to be done in order to reduce the impact of failure modes. The main purpose of this step is to remove the critical failure modes based on the company risk appetite. The action plan is differentiated based on the purpose of each action, whether to reduce the severity, occurrence, or detection. There are four types of action in responding the failure mode or risk (Niedbala, 2020).

   a. Avoid risk, is done if the score of severity, occurrence, and detection are very high that will cause significant harm, especially in finance. Thus, it is better not to take the risk at all. Instead of doing things that have those risks, the organization have to decide the alternative way to replace the initial process.
   b. Mitigate risk, is done if the score of severity, occurrence, and detection are relatively high but the treatment is still affordable and has lower cost than the impact. Mitigating risk cannot totally remove the risk. It only able to reduce the impact that might occur.
   c. Transfer risk is done if handling it alone has higher impact than share it to the third party. Mostly, these risks are unlikely happen.
   d. Accept risk, is done if the treatment of this risk is more costly than do nothing. Usually, it happens in a minor risk that has low score of severity, occurrence, and detection.

10. Calculate the resulting RPN as the failure modes are reduced or eliminated.

    This step is an evaluation action that has a purpose to measure how well the treatment of the risks. There will be rooms for continuous improvement if the impact of the treatment does not meet the expectation. It is done by reassess the score of severity, occurrence, and detection, then recalculate the RPN.

2.7 Benefit Cost Ratio

Benefit cost ratio is a method that is used to evaluate all the potential costs and revenues that an organization or company might generate from a project (Kenton, 2020). The outcome of this method is to measure whether the project is financially feasible, or the company have to change or modify the project. This analysis is considering all costs involved and possible profits to allows the organization in making better decision (The Economic Times, 2020). It takes both quantitative and qualitative factors into the analysis. The good thing about benefit cost ratio is that it helps the organization to interpret the inherent riskiness of forecasted net cash flows and profitability. Here are the steps of doing benefit cost ratio (Sebastian, 2021).

2.7.1 Present Value of Benefits

In calculating the value of benefits, here are the costs that commonly involved (Kenton, 2020).

1. The increasing of revenue and sales.
2. Intangible benefits, such as improved employee safety, customer satisfaction, and others.
3. Competitive advantage or market share.

The sum of the benefits will be calculated in a form of present value or the sum of discounted benefits. Here is the formula of the present value of benefits (Sebastian, 2021).

$$PV\ [Benefits] = \sum_{t=0}^{N} \frac{CF_t[Benefits]}{(1+i_t)^t} \quad (2\text{-}2)$$

where:

CF = Cash Flow of a period (classified as benefits)

i = Discount Rate or Interest Rate

N = Total Number of Periods

t = Period in which the Cash Flow occur

2.7.2 Present Value of Costs

In calculating the value of costs, here are the costs that commonly included (Kenton, 2020).

1. Direct cost that consists of direct labor that spent on manufacturing, inventory, raw materials, and manufacturing expenses.
2. Indirect cost that includes electricity and overhead cost form management, rent, and utilities.
3. Intangible cost that related with impact on customers, employees, and deliveries.
4. Opportunity cost, such as alternative investments and buy or make decision.
5. Cost of potential risks, such as regulatory risks, competition, and environmental impacts.

The sum of costs will be transformed into the present value of costs or the sum of discounted costs. The difference is that costs use the outflows while benefits use inflows. Here is the formula of the present value of costs (Sebastian, 2021).

$$PV\ [Costs] = \sum_{t=0}^{N} \frac{CF_t[Costs]}{(1+i_t)^t} \quad (2\text{-}3)$$

where:

CF = Cash Flow of a period (classified as costs)

i = Discount Rate or Interest Rate

N = Total Number of Periods

t = Period in which the Cash Flow occur

2.7.3 Ratio of Both Values

The last step is calculating the benefit cost ratio with the inputs of present value of benefits and present value of costs. Here is the formula (Sebastian, 2021).

$$Benefit\ Cost\ Ratio = \frac{|Present\ Value\ [Benefits]|}{|Present\ Value\ [Cost]|} \quad (2\text{-}4)$$

The result of this calculation will have three interpretations. Here is the summary of all the interpretations of benefit cost ratio.

Table 2.4 Interpretations of Benefit Cost Ratio

Value Range of Benefit Cost Ratio	**Generic Interpretation**
BCR < 1	Project generates losses
BCR = 1	Project is neither profitable nor lossy
BCR > 1	Project is profitable

(Source: Sebastian, 2021)

CHAPTER 3
METHODOLOGY

In this chapter, there will be flowchart and explanation of the flowchart about the step by step of methodology that is used in this research. The methodology contains the flow of the research starts from data collection, data processing, data analysis and interpretation, and drawing conclusion and suggestion.

3.1 Flowchart of Research Methodology

In this sub-chapter, the steps of this research will be mentioned in a form of flowchart. Here is the flowchart of the research steps.

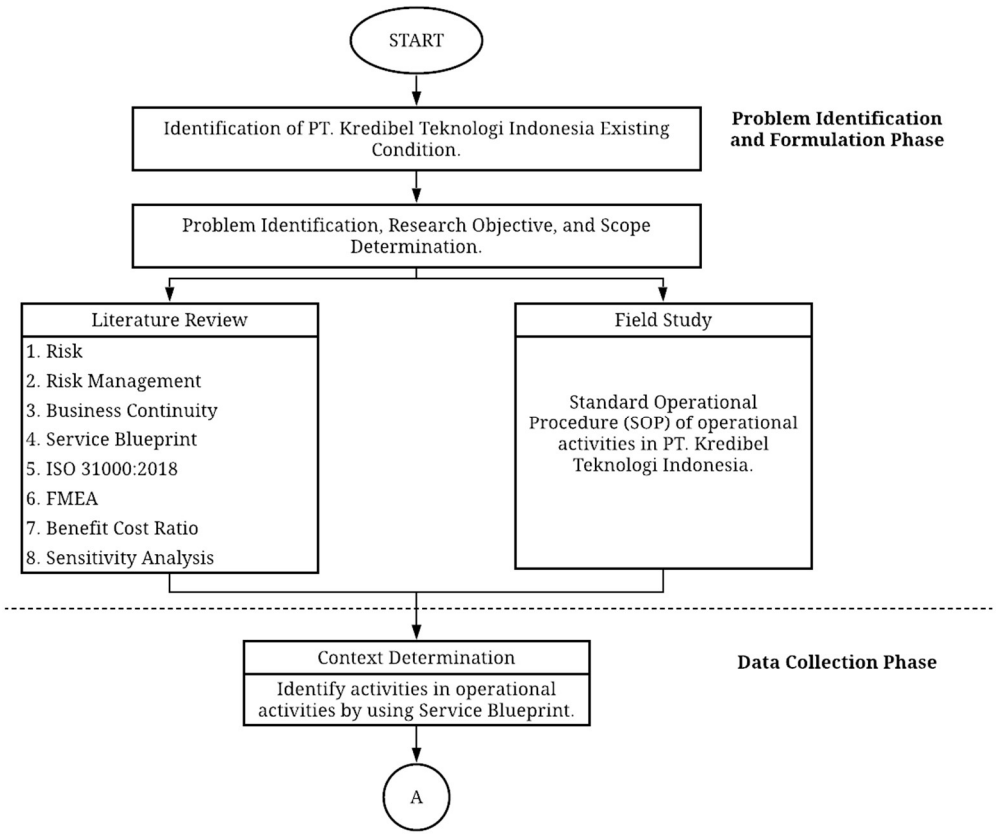

Figure 3.1 Research Methodology Flowchart

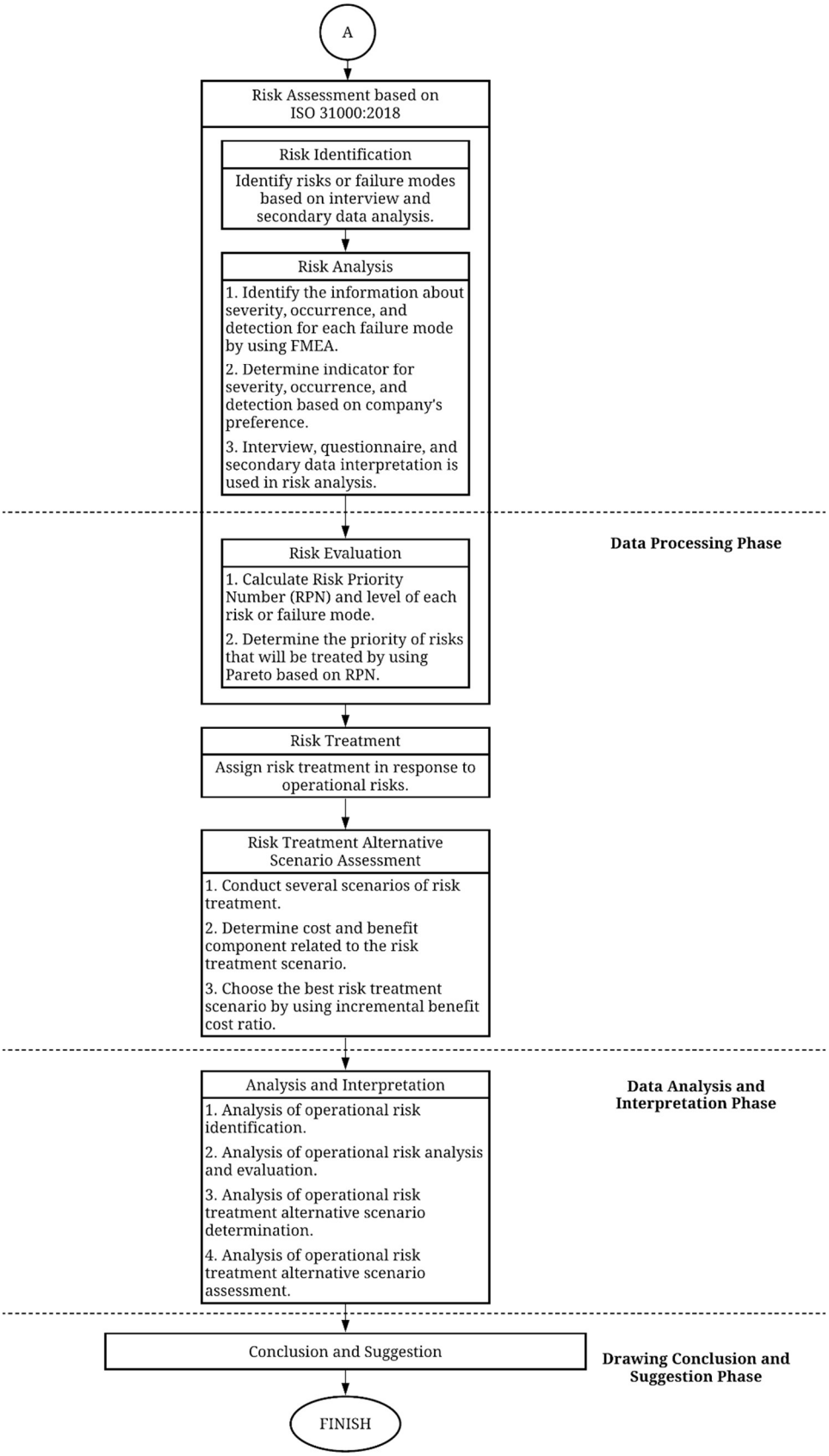

Figure 3.1 Research Methodology Flowchart

3.2 Description of Research Methodology

In this sub-chapter, there will be explanation of the flowchart that consists of steps that will be done in this research.

3.2.1 Problem Identification and Formulation Phase

This phase consists of identification of PT Kredibel Teknologi Indonesia existing condition. After the existing condition is being identified, the problem, objective, and scope of the research can be formulated. Then, literature review and field study are done to complete this phase. Here is the explanation of each part of this phase.

1. Identification of PT Kredibel Teknologi Indonesia Existing Condition

   In this part, the author identifies the existing condition of the company by directly doing an interview with the company. It has an aim to understand what the company needs in term of risk management.

2. Problem Identification, Research Objective, and Scope Determination

   In this part, there will be determination of the main problem of this research. The problem is based on the existing condition of the company. After that, the objective of the research will be identified, as well as the research scope that includes assumption and limitation. These three have to be determined in the beginning of the research to prevent the expansion of the problem.

3. Literature Review and Field Study

   In this part, literature review has to be done as the basis of the research. It includes method and supporting theories, which are Service Blueprint, risk, risk management, business continuity, ISO 31000:2018, FMEA, and Benefit Cost Ratio. While field study is done by gathering data that is provided by the company about the detail of the activities. It also equipped with direct interview with the company.

3.2.2 Data Collection Phase

This phase consists of context determination to define the detail of the activities that will be observed in the risk management. After that, risk will be identified based on the Service Blueprint, as well as the analysis of each risk. Here is the explanation of each part of this phase.

1. Context Determination

   In this part, the context of the research is done through analysis of given data and a direct interview to the company. It is done to make sure there will be no risk missed in the risk identification. The scope of this research will be the operational activities that refers to the service that is offered by the company. The activities will be mapped by using Service Blueprint, so that the detail of the activities will be clearly defined.

2. Risk Identification

   In this part, the risks or failure modes will be identified based on the activities that already determined in context determination. This part will be done by reviewing the document that given by the company. The document that is used is Standard Operational Procedure of operational activities in PT Kredibel Teknologi Indonesia. The risk that is identified refers to event that possibly occur and may disrupt the activities related to providing the service. Then, the risks will be reviewed and validated by the Head of Business of PT Kredibel Teknologi Indonesia. It is done to make sure that all the risks identified is relevant with the activities that are being observed. Here is the form that will be used to validate the risks.

Table 3.1 Risk Validation Form

No.	Activity	Risk	Validation		If valid		Notes (If not valid)
			Valid	Not Valid	Ever happened	Never happen	

3. Risk Analysis

In this part there will be information gathered that will be used as the basis of the severity, occurrence, and detection determination. The process will use FMEA approach. The scale will be made after doing direct interview and document interpretation and then will be validated by the Head of Business of PT Kredibel Teknologi Indonesia. After that, the respondent that is highly related to the operational activities and considered as expert is required to assess the severity, occurrence, and detection score through a questionnaire. The score given will be approved by the Director of the company. The company is highly involved in this part to make sure that the gathered data is valid. Here is the form that will be used to validate the risk score indicator and to assess each risk score.

Table 3.2 Risk Score Indicator Validation Form

No.	Aspect	Scale	Description	Validation		Notes (If not valid)
	Severity/ Occurrence/ Detection			Valid	Not valid	

Table 3.3 Risk Score Assessment Form

Activity Code	Activity	Risk Code	Risk	Risk Impact	Severity Score	Risk Cause	Occurrence Score	Risk Detection	Detection Score
					Filled by respondent		Filled by respondent		Filled by respondent

3.2.3 Data Processing Phase

In this phase, all data that is gathered in the previous phase will be processed. The first part is risk evaluation that will consider the company preferences. After that, in response of the risks, the risk treatment alternative scenario will be conducted. Then, there will be assessment of risk treatment alternative scenarios. Here is the explanation of each part of this phase.

1. Risk Evaluation

   In this part, the author will calculate Risk Priority Number (RPN) and level based on the data in previous phase. The risks will be classified as priority risks by using Pareto and considering the RPN of each risk. Here is the formula that is used to calculate RPN based on 2.6.

$$RPN = Severity\ x\ Occurrence\ x\ Detection \quad (2\text{-}1)$$

2. Risk Treatment Alternative Scenario Determination

   In this part, the risk treatment alternative scenario will be conducted as response to the risks. The treatment selection will be based on the result of risk evaluation and the preferences of the company. The treatment can be either avoid, mitigate, transfer, or accept. Avoid is to replace the activities, mitigate is to reduce the impact of the risk, transfer is to share the risk to a third party, and accept is to do nothing because the treatment is more costly than the impact of the risk.

3. Risk Treatment Alternative Scenario Assessment

   In this part, the whole cost component that will be used if the risk treatment scenario is implemented will be calculated and compared with the whole benefit that will be obtained. The cost component is defined from the cost that is directly used to implement the scenario. The benefit is determined by defining what factor that is directly improved by doing those treatment, then it will be equivalented into Indonesian Rupiah. Both cost and benefit components are based on the company's preference. Here is the formula of Benefit Cost Ratio based on 2.7.3.

$$Benefit\ Cost\ Ratio = \frac{|Present\ Value\ [Benefits]|}{|Present\ Value\ [Cost]|} \quad (2\text{-}4)$$

   This part is done to determine whether the risk treatment scenario is feasible to be implemented and choose the scenario that has the highest benefit cost ratio as the risk treatment recommendation. Here are the table that will be used to determine the benefit and cost component of each risk treatment.

Table 3.4 Benefit Component Validation Form

Risk Code	Risk	Risk Treatment			Benefit Component	
		Type	Action	To reduce	Component	Proxy
		Avoid/ Mitigate		Severity/ Occurrence/ Detection		

Table 3.5 Cost Component Validation Form

Risk Code	Risk	Risk Treatment			Cost Component			
		Type	Action	To reduce	CAPEX	CAPEX Proxy	OPEX	OPEX Proxy
		Avoid/ Mitigate		Severity/ Occurrence/ Detection				

3.2.4 Data Analysis and Interpretation Phase

In this phase, there will be analysis and interpretation of the result from data collection and processing. The analysis will be differentiated into analysis of the risk identification, analysis of the risk assessment, analysis of the risk treatment recommendation, and analysis of the risk treatment alternative assessment as the final part of the data processing.

1. Operational Risk Identification

   In this part, the analysis starts from the risk management scope determination until the risk identification from each operational process.

2. Operational Risk Analysis and Evaluarion

   In this part, the analysis consists of the risk analysis and risk evaluation. The risk analysis consists of how the cause, impact, and control are being identified and how the process and result of severity, occurrence, and detection rating assessment. The risk assessment consists of how the calculation and result of Risk Priority Number (RPN) that leads to risk ranking and risk priority.

3. Operational Risk Treatment Alternative Scenario Determination

   In this part, the analysis covers the process of risk treatment alternatives determination as well as the scenarios determination based on the treatment alternatives that already assigned to every risk.

4. Operational Risk Treatment Alternative Scenario Assessment

   In this part, the analysis consists of the calculation process as well as the result of benefit cost ratio towards the risk treatment alternative scenario.

3.2.5 Drawing Conclusion and Suggestion Phase

The last phase of this research will be a phase of making conclusion according to the whole process that is done by the author. The conclusion is conducted to answer the objective of the research. Besides, in this phase there will be suggestion that is formulated for PT Kredibel Teknologi Indonesia as the observed object and also for further similar research.

(This page is intentionally left blank)

CHAPTER 4
DATA COLLECTION AND PROCESSING

In this chapter, there will be explanation about result of data collection and the process of the research based on the objectives and methodology that already mentioned in the previous chapter.

4.1 General Description and Company Profile

PT Kredibel Teknologi Indonesia or commonly called Kredibel is a company that highly rely on big data to provide their service. This company is established in March 2016 and have a vision to reduce the potency of fraud case in online shopping ecosystem based on people's report by doing identification activity. Previously, this company was called Penipu.id but then changed become Kredibel with several considerations.

PT Kredibel Indonesia is the first profit company that focus on reducing potential online fraud. It is a B2B and B2C company. Their B2B product that already established is called Fraud Management System (FMS). While for B2C product is a free service called "Cek Rekening Penipu Online". This service provides user to check any bank account number or mobile phone number if they ever get a complaint based on Kredibel databease. This can be used by only making an account in their website. By making a Kredibel account, the user also can report any transaction that happen with the fraudster to Kredibel. Their B2C product only competitor is a website that managed by Indonesian Government, specifically Kementerian Komunikasi dan Informasi, called CekRekening.id. While for their B2B service, they still do not have any competitor yet. Kredibel has hundred thousands of fraud case in their database.

Since Kredibel is a start-up company, they only have two main departments in their organizational structure. The first department is Business Department that consists of two functions, which are Marketing & Sales and also Operation. Each function also consists of several staff. Marketing & Sales consists of marketing staff and sales staff, while Operation consists of legal staff, finance staff, human resource staff, and general affair staff. The second department is Product Engineering

Department that consists of three different functions, which are Research & Development, Engineering, and IT Security. These functions also have several staffs. Research and Development consists of AI staff and data analyst staff. Engineering consists of front-end staff, back-end staff, mobile developer, and UI/UX staff. IT Security consists of Development and Operation (DevOps) and IT security staff. Here is the detailed organizational structure of PT Kredibel Teknologi Indonesia.

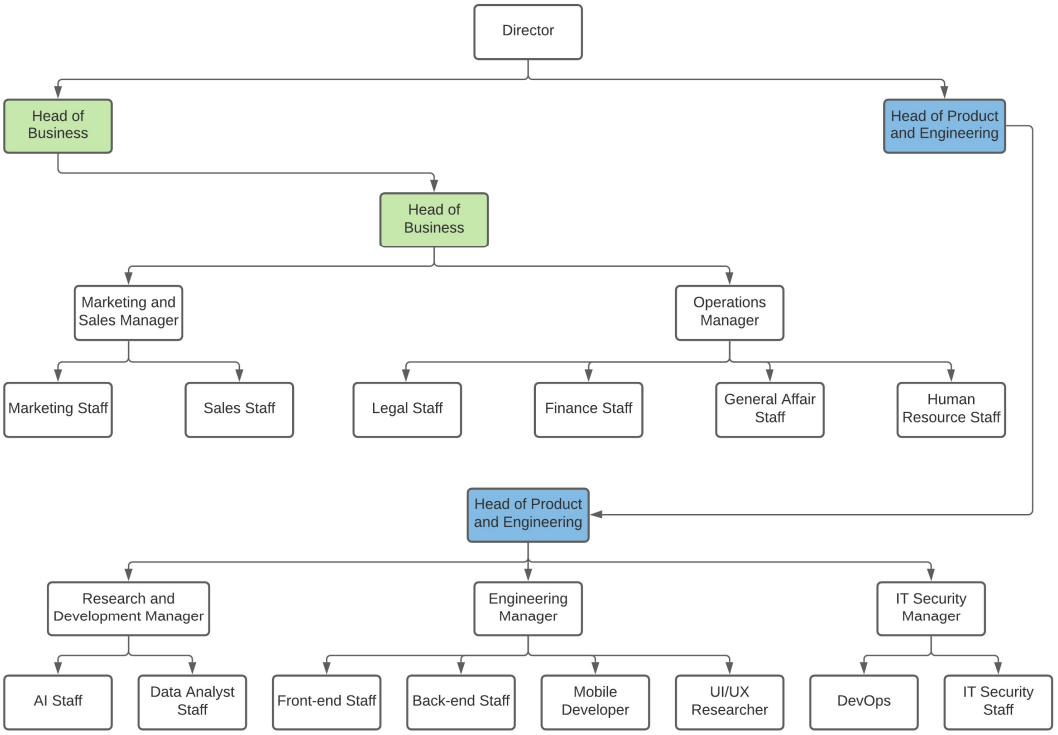

Figure 4.1 Kredibel Organizational Structure

(Source: PT Kredibel Teknologi Indonesia, 2016)

4.2 Operational Activities Identification

In this sub-chapter, there will be identification of the observed process. This step is done as the context determination process of risk management. The process that is observed consists of operational activities of PT Kredibel Teknologi Indonesia, which is their service called Fraud Management System. It is a Business to Business (B2B) service that has an aim to prevent any fraud case. This service highly depends on the fraud information data that the company has. It is divided into three part which are data gathering, contract agreement, and service fulfillment. Since the observed process is a service, the identification is using Service Blueprint

framework. In service blueprint the activities will be differentiated into five parts, which are physical evidence, customer action, onstage action, backstage action, and support process. However, only risks of customer action, onstage action, and backstage action that will be identified as the company responsibility.

This research's observed object is the offered service, which called Fraud Management System (FMS). It is chosen as the observed object to maximize the profit by minimizing the error that are mostly caused by human error since Kredibel is a startup company. This service's main activities are related to the database making that later on will be used by the clients. There are two kinds of Kredibel's customers, which are users that are report the fraud and clients that are used the database filled with fraud report. Thus, the value proposition of Fraud Management System is the data itself. By using the database, clients are able to check the integrity of their own users. However, information about which users that are being checked by the client is included as restricted information for Kredibel. In other word, Kredibel only provide the database and the client have to buy some kind of credit or billing to check their user. The billing is counted every user that is being checked. The whole process of Fraud Management System excluded the website system making is differentiated into three parts, which are data gathering, contract agreement, and service fulfillment. Here is the explanation of each part of the service.

4.2.1 Data Gathering

Data gathering is a process when the company gather the data of fraud information from the public. The process is done by the public individually and voluntarily. First, the user has to visit Kredibel's website and login to their account. A welcome interface will be seen, and the website will be the physical evidence. After that, the user will visit a specific page called "Laporkan Penipuan" then another welcome interface will be seen. In this page, there will be a procedure to submit information about fraud case as the physical evidence. Last, the user will fill the form and submit the fraud information. Kredibel will verify this information whether it is valid or not.

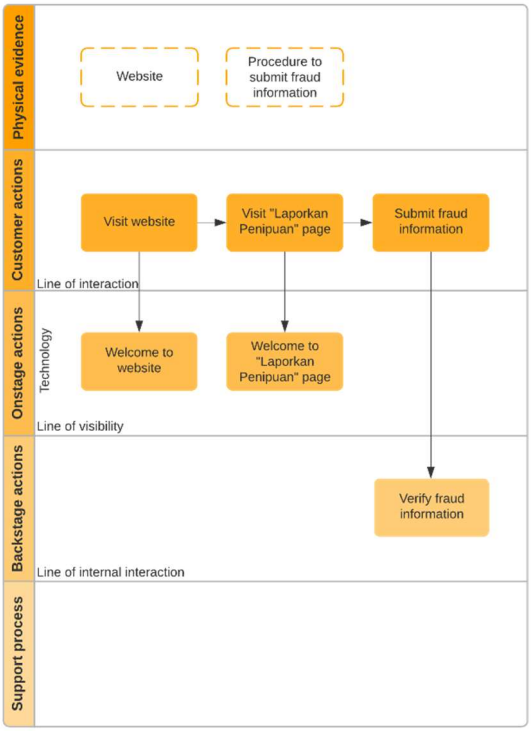

Figure 4.2 Data Gathering Service Blueprint

Table 4.1 Data Gathering Activities

Activity Code	Activity
A-1.1	Visit website
A-1.2	Visit “Laporkan Penipuan” page
A-1.3	Submit fraud information
A-2.1	Welcome to website
A-2.2	Welcome to “Laporkan Penipuan” page
A-3.1	Verify fraud information

4.2.2 Contract Agreement

Contract agreement is done before the client is able to use the service in order to match the client’s requirement, provider’s terms and condition, and the price. First, the customer visit Kredibel’s website then they will see a welcome interface and the physical evidence is the website. After that, the customer has to visit a page for enterprise then they also will see another welcome interface. In this action, the description of the service will be the physical evidence. Next, the

customer or can be called client can request a demo by filling their information based on their needs. Once, Kredibel accept the request, an email that contains demo day schedule request will be sent to the client and the client's information is the physical evidence. Then, the request has to be approved by the client. Thus, the physical evidence will be the demo day request. The next activity is both client and provider prepare a requirement, terms, and condition that will be discussed in the Demo Day. Once they both agreed, a non-disclosure agreement will be made. Last, the client will get API key to use the service. The client has to pay for the billing at price that previously agreed, and the API key will be the physical evidence of this activity.

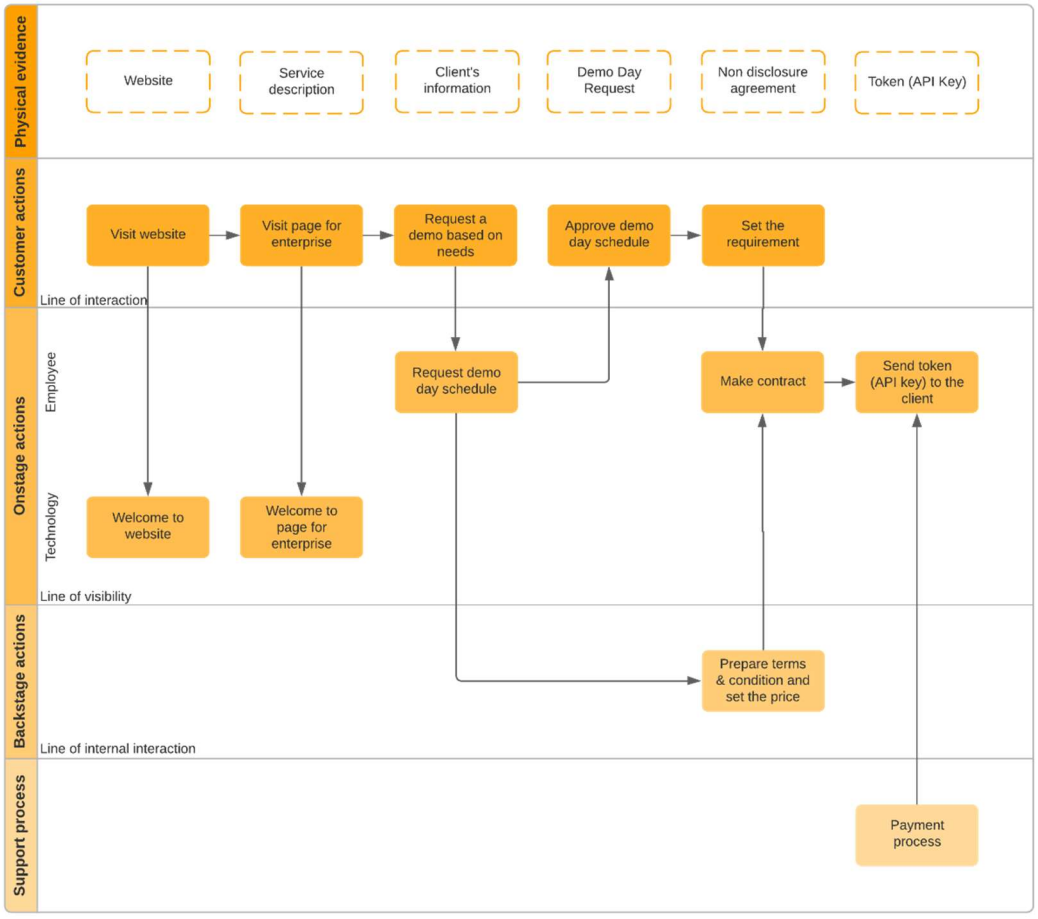

Figure 4.3 Contract Agreement Service Blueprint

Table 4.2 Contract Agreement Activities

Activity Code	Activity
B-1.1	Visit website
B-1.2	Visit page for enterprise
B-1.3	Request a demo based on needs
B-1.4	Approve demo day schedule
B-1.5	Set the requirement
B-2.1.1	Request demo day schedule
B-2.1.2	Make contract
B-2.1.3	Send API key to the client
B-2.2.1	Welcome to website
B-2.2.2	Welcome to page for enterprise
B-3.1	Prepare terms & condition and set the price

4.2.3 Service Fulfillment

Service fulfillment is when the client uses the service itself. The process is done by screening the information that is entered by the client and the output will be an information if there are any fraud historical cases regarding a mobile phone or a bank account number. First, the client inserts the API key that previously given by Kredibel. A confirmation message will be sent to the client as the physical evidence. After that the client have to refill the billing so that they can use the service. There also will be a confirmation message once the billing is inputted to the system. Then the client can simply input the query in the form of user identity, bank account number, or mobile number to the system. The system will do the screening process based on company database and the result will be sent to the client as the physical evidence.

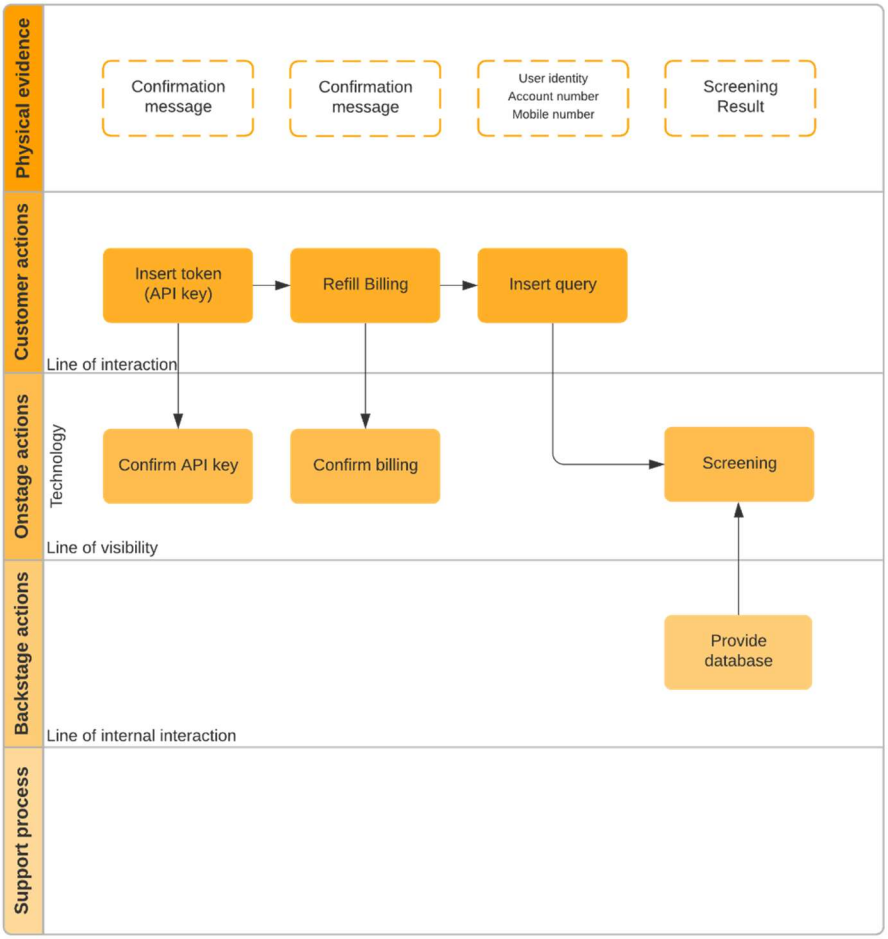

Figure 4.4 Service Fulfillment Service Blueprint

Table 4.3 Service Fulfillment Activities

Activity Code	Activity
C-1.1	Insert API key
C-1.2	Refill billing
C-1.3	Insert query
C-2.1	Confirm API key
C-2.2	Confirm billing
C-2.3	Screening
C-3.1	Provide database

4.3 Operational Risk Identification

Operational risk identification in PT Kredibel Teknologi Indonesia is done by using Failure Mode and Effect Analysis (FMEA) and supported with direct interview to the company representative which is the Head of Business and document review and interpretation. Documents that are being reviewed are Service Operational Procedure (SOP), risk management of data and information security based on ISO 27001, and draft of non-disclosure agreement. Then, the identified risk is validated by the company. The operational risk identification validation questionnaire can be seen in **Attachment 1**. The identified risks are the potential failures that can give bad impact to the company's operational activity. The identification is based on activities that are already determined previously in service blueprint. The risks are differentiated based on the source of risk, which are user/client, system, and employee. The differentiation is done to make sure there is no risk missed during the risk identification. Here is the result of operational risk identification in PT Kredibel Teknologi Indonesia.

Table 4.4 Kredibel Operational Risk

Process	Activity Code	Activity	Risk Source	Risk Code	Risk
Data Gathering	A-1.1	Visit website	System	R1	The website cannot be accessed by user
	A-2.1	Welcome to website	User/Client	R2	The user finds it hard to find "Laporkan Penipuan" button
	A-1.2	Visit “Laporkan Penipuan” page	User/Client	R3	The user makes mistake in filling out the report form
				R4	The report submitted is less detailed
			System	R5	"Laporkan Penipuan" page cannot be accessed by user
	A-2.2	Welcome to “Laporkan Penipuan” page	User/Client	R6	The user does not understand how to fill the form
	A-1.3	Submit fraud information	User/Client	R7	The report accidentally submitted when it is not finished yet
			System	R8	The report cannot be submitted
				R9	The report is submitted but not recorded in the database
	A-3.1	Verify fraud information	Employee	R10	The fake/wrong report is verified
				R11	The real/good report is not verified

Process	Activity Code	Activity	Risk Source	Risk Code	Risk
Contract Agreement	B-1.1	Visit website	System	R12	The website cannot be accessed by client
	B-2.2.1	Welcome to website	User/Client	R13	The client finds it hard to find "Enterprise" button
	B-1.2	Visit page for enterprise	System	R14	The client failed to login
	B-2.2.2	Welcome to page for enterprise	User/Client	R15	The client does not understand the description of the service
	B-1.3	Request a demo based on needs	User/Client	R16	The submitted needs are less detailed
				R17	The submitted needs is not clear
	B-2.1.3	Request demo day schedule	Employee	R18	The proposed date is not approved by the client
	B-1.4	Approve demo day schedule	Employee	R19	The email is forgotten to be sent
				R20	There is a mistake in email
			System	R21	The email is sent but not arrive to the client
				R22	The email goes to spam folder
	B-1.5	Set the requirement	Employee	R23	The proposed requirement from the client cannot be fulfilled by Kredibel
				R24	There is a misperception toward the needs

Process	Activity Code	Activity	Risk Source	Risk Code	Risk
	B-2.1.2	Make contract	User/Client	R25	The client does not understand how the service run
			Employee	R26	There is mistake inside the contract
				R27	Kredibel is failed to fulfill the agreed requirement
	B-3.1	Prepare terms & condition and set the price	Employee	R28	The terms & condition are not approved by the client
				R29	The terms & condition bring harm to Kredibel
				R30	There are some factors that is forgotten to consider
	B-2.1.3	Send API key to the client	Employee	R31	API key is given late
Service Fulfillment	C-1.1	Insert API key	User/Client	R32	The client does not understand how to insert API Key
			System	R33	API Key cannot be used
	C-2.1	Confirm API key	System	R34	The API Key confirmation is not sent
	C-1.2	Refill billing	User/Client	R35	The client does not understand how to refill billing

Process	Activity Code	Activity	Risk Source	Risk Code	Risk
			System	R36	Billing cannot be used
	C-2.2	Confirm billing	System	R37	The billing confirmation is not sent
	C-1.3	Insert query	User/Client	R38	The client makes mistake in inserting query
	C-2.3	Screening	User/Client	R39	The client cannot understand the screening report
			Employee	R40	There is error in screening report
	C-3.1	Provide database	System	R41	There is no sufficient data/the data is less accurate
				R42	The real/non-fraudster account classified as fake/fraudster account
				R43	The fake/fraudster account classified as real/non-fraudster account

4.4 Operational Risk Analysis

After operational risks are being identified, the next step based on ISO 31000:2018 is risk analysis. Operational risk analysis based on FMEA is done by identifying the cause, impact, and control of each risk. Then, severity, occurrence, and detection score are given to each risk based on the identified cause, impact, and control.

4.4.1 Risk Cause, Impact, and Control Identification

Based on operational risk identification in sub-chapter 4.3, there are 43 operational risks in the activities that are related to the service offered. The cause, impact, and control are identified for every risk by using direct interview to the Head of Business and document review and interpretation. Documents that are being reviewed are Service Operational Procedure (SOP), risk management of data and information security based on ISO 27001, and draft of non-disclosure agreement. Here is the result of cause, impact, and control risk identification in PT Kredibel Teknologi Indonesia.

Table 4.5 Kredibel Risk Cause, Impact, and Control

Risk Code	Risk	Risk Impact	Risk Cause	Risk Control
R1	The website cannot be accessed by user	Reduce user experience	Lack of website treatment procedure	None
R2	The user finds it hard to find "Laporkan Penipuan" button	Reduce user experience	Bad UI/UX	UI/UX evaluation (not routine and not documented)
R3	The user makes mistake in filling out the report form	Reduce number of valid reports	The form instruction is less informative	None
R4	The report submitted is less detailed	Reduce number of valid reports	The form instruction is less informative	None

Risk Code	Risk	Risk Impact	Risk Cause	Risk Control
R5	"Laporkan Penipuan" page cannot be accessed by user	Reduce user experience	Lack of website treatment procedure	None
R6	The user does not understand how to fill the form	Reduce number of valid reports	The form instruction is less informative	None
R7	The report accidentally submitted when it is not finished yet	Reduce number of valid reports	Bad UI/UX	None
R8	The report cannot be submitted	User cancels submit the report	Lack of website treatment procedure	Website checking (not routine and not documented)
R9	The report is submitted but not recorded in the database	Reduce number of valid reports	Lack of website treatment procedure	None
R10	The fake/wrong report is verified	Reduce data reliability	Lack of report standardization	None
R11	The real/good report is not verified	Reduce data reliability	Lack of report standardization	None
R12	The website cannot be accessed by client	Reduce customer experience of client	Lack of website treatment procedure	None

Risk Code	Risk	Risk Impact	Risk Cause	Risk Control
R13	The client finds it hard to find "Enterprise" button	Reduce customer experience of client	Bad UI/UX	UI/UX evaluation (not routine and not documented)
R14	The client failed to login	Reduce number of clients	Lack of website treatment procedure	None
R15	The client does not understand the description of the service	Reduce number of clients	The website is less informative	Client's feedback after dealing process
R16	The submitted needs are less detailed	The service is not matched with the client	The needs instruction is less informative	None
R17	The submitted needs is not clear	Lengthen the agreement process	The needs instruction is less informative	None
R18	The proposed date is not approved by the client	Lengthen the agreement process	Lack of date determination procedure	None
R19	The email is forgotten to be sent	Client cancels using the service	Lack of service operation procedure	Approval email checking (before sending the email)

Risk Code	Risk	Risk Impact	Risk Cause	Risk Control
R20	There is a mistake in email	Client cancels using the service	Lack of email making procedure	Approval email checking (before sending the email)
R21	The email is sent but not arrive to the client	Client cancels using the service	Lack of approval email monitoring	None
R22	The email goes to spam folder	Client cancels using the service	Lack of approval email monitoring	None
R23	The proposed requirement from the client cannot be fulfilled by Kredibel	Client cancels using the service	Lack of the need's standardization	None
R24	There is a misperception toward the needs	The service is not matched with the client	Lack of the need's standardization	Historical agreement evaluation (not routine and not documented)
R25	The client does not understand how the service run	Client cancels using the service	Bad service description	Client feedback
R26	There is mistake inside the contract	Delay the service usage	Lack of service operation procedure	Contract controlling before it is given to the client

Risk Code	Risk	Risk Impact	Risk Cause	Risk Control
R27	Kredibel is failed to fulfill the agreed requirement	Client stops using the service	Lack of service operation procedure	Status of service monitoring (continues)
R28	The terms & condition are not approved by the client	Lengthen the agreement process	Lack of terms & condition making procedure	None
R29	The terms & condition bring harm to Kredibel	Higher cost	Lack of terms & condition making procedure	Compare with historical agreement (not routine and not documented)
R30	There are some factors that is forgetten to consider	Lengthen the agreement process	Lack of terms & condition making procedure	Compare with historical agreement (not routine and not documented)
R31	The API key is given late	Delay the service usage	Lack of employee training	Employee monitoring (continues)
R32	The client does not understand how to insert API Key	The service cannot be used	Bad service usage instruction	None

Risk Code	Risk	Risk Impact	Risk Cause	Risk Control
R33	API Key cannot be used	The service cannot be used	Lack of API Key treatment procedure	API Key monitoring (continues)
R34	The API Key confirmation is not sent	Reduce customer satisfaction of client	Lack of service operation procedure	None
R35	The client does not understand how to refill billing	The service cannot be used	Bad service usage instruction	Client feedback (not routine)
R36	Billing cannot be used	The service cannot be used	Lack of billing treatment procedure	None
R37	The billing confirmation is not sent	Reduce customer satisfaction of client	Lack of service operation procedure	None
R38	The client makes mistake in inserting query	The service cannot be used	The service usage instruction is less informative	Client feedback (not routine)
R39	The client does not understand the screening report	Reduce customer satisfaction of client	The screening report is hard to understand	Client feedback (not routine)
R40	There is error in screening report	The service cannot be used	Lack of dashboard treatment procedure	None
R41	There is no sufficient data/the data is less accurate	Client stops using the service	Lack of data	None

Risk Code	Risk	Risk Impact	Risk Cause	Risk Control
R42	The real/non-fraudster account classified as fake/fraudster account	Client stops using the service	Bad data screening procedure	None
R43	The fake/fraudster account classified as real/non-fraudster account	Client stops using the service	Bad data screening procedure	None

4.4.2 Severity, Occurrence, and Detection Rating Assessment

Severity, occurrence, and detection rating assessment is taken from questionnaire. The questionnaire is filled by three respondents that are considered as expert and directly related to the service, so the judgement is valid. The used rating indicator is already validated previously by the company's representative to make sure that the criteria is matched with the company preference. The operational risk score rating validation questionnaire can be seen in **Attachment 2**. Here are the severity, occurrence, and detection scoring indicator that is used in this risk management.

Table 4.6 Severity Scoring Indicator

Severity		
Category	**Description**	**Rating**
Extreme	Risk can cause major disruption to service fulfillment (all service fulfillment stops)	5
Heavy	Risk can cause major disruption to service fulfillment (give impact on most of the service fulfillment processes, the service provided do not meet quality standards and require repetition of several aspects of the service).	4
Medium	Risk can cause moderate disruption to service fulfillment (give impact on several service fulfillment processes, and the service provided do not meet quality standards)	3
Light	Risk can cause moderate disruption to service fulfillment (give impact on related process, the service provided is slightly below quality standards but can be fixed)	2
Insignificant	Risk may cause minor interruptions that do not have a significant impact on service quality	1

Table 4.7 Occurrence Scoring Indicator

Occurrence		
Category	**Description**	**Rating**
Almost certain	Cause of risk can occur (based on experience for the past 3 months)	5
May occurred	Cause of risk can occur (based on experience from 3 months to 1 year ago)	4
Not common but can be occurred	Cause of risk can occur (based on experience from 1 year to 2 years ago)	3
Unlikely	Cause of risk can occur (based on experience from 2 years to 3 years ago)	2

Occurrence		
Category	**Description**	**Rating**
Much less likely	Cause of risk never occurs (based on experience for the past 3 years)	1

Table 4.8 Detection Scoring Indicator

Detection		
Category	**Description**	**Rating**
Almost impossible	The checking system has no possibility of detecting risk	5
High	The checking system has a low chance of detecting risk	4
Moderate	The checking system has a moderate chance of detecting risk	3
Low	The checking system has a high chance of detecting risk	2
Almost certain	The checking systems can almost certainly detect risk	1

By using those risk score rating indicator, respondent that are related directly to the service and considered as expert, which is the Head of Business are asked to give severity, occurrence, and detection rating for every risk based on the risk cause, impact, and control. The score given is known and approved by the Director of PT Kredibel Teknologi Indonesia. The operational risk score questionnaire can be seen in **Attachment 3**. Here is the result of severity, occurrence, and detection for every operational risk in PT Kredibel Teknologi Indonesia.

Table 4.9 Severity, Occurrence, and Detection Score of Kredibel Operational Risk

Risk Code	Risk	Severity Score (1-5)	Occurrence Score (1-5)	Detection Score (1-5)
R1	The website cannot be accessed by user	5	4	5
R2	The user finds it hard to find "Laporkan Penipuan" button	3	4	5
R3	The user makes mistake in filling out the report form	2	5	5
R4	The report submitted is less detailed	3	5	5
R5	"Laporkan Penipuan" page cannot be accessed by user	5	4	5
R6	The user does not understand how to fill the form	3	4	5
R7	The report accidentally	3	5	5

Risk Code	Risk	Severity Score (1-5)	Occurrence Score (1-5)	Detection Score (1-5)
	submitted when it is not finished yet			
R8	The report cannot be submitted	5	4	2
R9	The report is submitted but not recorded in the database	3	4	5
R10	The fake/wrong report is verified	3	5	5
R11	The real/good report is not verified	5	5	5
R12	The website cannot be accessed by client	4	4	5
R13	The client finds it hard to find "Enterprise" button	5	5	2
R14	The client failed to login	5	5	5

Risk Code	Risk	Severity Score (1-5)	Occurrence Score (1-5)	Detection Score (1-5)
R15	The client does not understand the description of the service	4	5	2
R16	The submitted needs are less detailed	4	5	5
R17	The submitted needs is not clear	4	5	5
R18	The proposed date is not approved by the client	3	5	5
R19	The email is forgotten to be sent	3	1	5
R20	There is a mistake in email	3	1	1
R21	The email is sent but not arrive to the client	3	1	5
R22	The email goes to spam folder	3	1	5

Risk Code	Risk	Severity Score (1-5)	Occurrence Score (1-5)	Detection Score (1-5)
R23	The proposed requirement from the client cannot be fulfilled by Kredibel	5	5	5
R24	There is a misperception toward the needs	3	5	5
R25	The client does not understand how the service run	3	5	5
R26	There is mistake inside the contract	3	4	5
R27	Kredibel is failed to fulfill the agreed requirement	5	1	5
R28	The terms & condition are not approved by the client	5	5	5
R29	The terms & condition	5	1	2

Risk Code	Risk	Severity Score (1-5)	Occurrence Score (1-5)	Detection Score (1-5)
	bring harm to Kredibel			
R30	There are some factors that is forgetten to consider	5	4	5
R31	The API key is given late	5	1	5
R32	The client does not understand how to insert API Key	5	1	5
R33	API Key cannot be used	5	1	5
R34	The API Key confirmation is not sent	3	1	5
R35	The client does not understand how to refill billing	3	1	5
R36	Billing cannot be used	5	1	5
R37	The billing confirmation is not sent	3	1	5

Risk Code	Risk	Severity Score (1-5)	Occurrence Score (1-5)	Detection Score (1-5)
R38	The client makes mistake in inserting query	1	1	5
R39	The client cannot understand the screening report	3	1	5
R40	There is error in screening report	5	5	5
R41	There is no sufficient data/the data is less accurate	5	5	5
R42	The real/non-fraudster account classified as fake/fraudster account	5	5	5
R43	The fake/fraudster account classified as real/non-fraudster account	5	5	5

4.5 Operational Risk Evaluation

The next step based on ISO 31000:2018 is risk evaluation. The risk evaluation is done by determining the Risk Priority Number (RPN) of every risk. Then, all of the risks are ranked based on the RPN. Finally, the priority operational risks are determined using Pareto.

4.5.1 Operational Risk Priority Number (RPN) Assessment

Risk Priority Number (RPN) is calculated by using **Formula (2-1)** in **Sub-chapter 2.6**. The highest possible RPN value is 125, which is the multiplication of 5 x 5 x 5. Here is the result of Risk Priority Number (RPN) assessment for every operational risk in PT Kredibel Teknologi Indonesia.

Table 4.10 Kredibel Risk Priority Number

Risk Code	Risk	Risk Priority Number
R1	The website cannot be accessed by user	100
R2	The user finds it hard to find "Laporkan Penipuan" button	60
R3	The user makes mistake in filling out the report form	50
R4	The report submitted is less detailed	75
R5	"Laporkan Penipuan" page cannot be accessed by user	100
R6	The user does not understand how to fill the form	60
R7	The report accidentally submitted when it is not finished yet	75
R8	The report cannot be submitted	40
R9	The report is submitted but not recorded in the database	60

Risk Code	Risk	Risk Priority Number
R10	The fake/wrong report is verified	75
R11	The real/good report is not verified	125
R12	The website cannot be accessed by client	80
R13	The client finds it hard to find "Enterprise" button	50
R14	The client failed to login	125
R15	The client does not understand the description of the service	40
R16	The submitted needs are less detailed	100
R17	The submitted needs is not clear	100
R18	The proposed date is not approved by the client	75
R19	The email is forgotten to be sent	15
R20	There is a mistake in email	3
R21	The email is sent but not arrive to the client	15
R22	The email goes to spam folder	15
R23	The proposed requirement from the client cannot be fulfilled by Kredibel	125
R24	There is a misperception toward the needs	75
R25	The client does not understand how the service run	75
R26	There is mistake inside the contract	60
R27	Kredibel is failed to fulfill the agreed requirement	25

Risk Code	Risk	Risk Priority Number
R28	The terms & condition are not approved by the client	125
R29	The terms & condition bring harm to Kredibel	10
R30	There are some factors that is forgetten to consider	100
R31	The API key is given late	25
R32	The client does not understand how to insert API Key	25
R33	API Key cannot be used	25
R34	The API Key confirmation is not sent	15
R35	The client does not understand how to refill billing	15
R36	Billing cannot be used	25
R37	The billing confirmation is not sent	15
R38	The client makes mistake in inserting query	5
R39	The client does not understand the screening report	15
R40	There is error in screening report	125
R41	There is no sufficient data/the data is less accurate	125
R42	The real/non-fraudster account classified as fake/fraudster account	125
R43	The fake/fraudster account classified as real/non-fraudster account	125

4.5.2 Operational Risk Ranking Determination

The rank of every risk is determined based on Risk Priority Number (RPN). The first ranked risk is the risk that has the highest RPN. The RPN also used to determine the level of the risk. The risk level is differentiated into four, which are extreme risk, high risk, medium risk, and low risk. Since Kredibel currently use risk management based on ISO 27001, the company apply risk level description with only two risk dimensions. Therefore, the author proposes risk level description with three risk dimensions that is suitable for Kredibel which included as a startup company. Here is the detail of risk level range determination.

Table 4.11 Risk Level Range Determination

Severity		Occurrence		Detection	
Rating	**Risk Level**	**Rating**	**Level**	**Rating**	**Level**
5	Extreme	5	High	5	Medium
4	High	4	Medium	4	Low
3	Medium	3	Medium	3	Low
2	Medium	2	Medium	2	Low
1	Low	1	Low	1	Low

Based on the table above, risks with severity score, occurrence score, and detection score of 5 are included as extreme risks. Risks with severity score of 4 and occurrence score and detection score of 5 are included as high risks. Risks with severity score of 3, occurrence score of 4, and detection score of 5 are included as medium risk. The range determination is mostly based on the severity, which is the impact that company can get if the risks are happened. Risks with severity score of 4 and 5 are risks that are included as risks that must be treated. While for the occurrence score, only risks with the occurrence score of 5 or risks that are ever happened in the past 3 months that are included as risks that must be treated to maximize the effectivity of the cost usage. Finally, the detection score is not highly being concerned because most of the risks are risks that are hard to detect. After the risks are being classified into several risks, risk treatments are assigned to each risk. High and extreme risks are risks that later on have to be treated. Here is the

recapitulation of description of each level of risk in a form of RPN value range, also the result of operational risk ranking determination in PT Kredibel Teknologi Indonesia.

Table 4.12 Risk Level Description

Risk Level	RPN Value
Extreme	RPN > 100
High	60 > RPN >= 100
Medium	20 > RPN >= 60
Low	RPN < 20

Table 4.13 Operational Risk Ranking (Ascendant)

Risk Code	Risk	Risk Priority Number	Risk Level	Percentage of Total RPN	Accumulated Percentage
R11	The real/good report is not verified	125	Extreme	4,63%	4,63%
R14	The client failed to login	125	Extreme	4,63%	9,27%
R23	The proposed requirement from the client cannot be fulfilled by Kredibel	125	Extreme	4,63%	13,90%
R28	The terms & condition are not approved by the client	125	Extreme	4,63%	18,53%

Risk Code	Risk	Risk Priority Number	Risk Level	Percentage of Total RPN	Accumulated Percentage
R40	There is error in screening report	125	Extreme	4,63%	23,17%
R41	There is no sufficient data/the data is less accurate	125	Extreme	4,63%	27,80%
R42	The real/non-fraudster account classified as fake/fraudster account	125	Extreme	4,63%	32,43%
R43	The fake/fraudster account classified as real/non-fraudster account	125	Extreme	4,63%	37,06%
R1	The website cannot be accessed by user	100	High	3,71%	40,77%
R5	"Laporkan Penipuan" page cannot be accessed by user	100	High	3,71%	44,48%
R16	The submitted needs are less detailed	100	High	3,71%	48,18%
R17	The submitted needs is not clear	100	High	3,71%	51,89%
R30	There is some factors that is forgetten to consider	100	High	3,71%	55,60%
R12	The website cannot be accessed by client	80	High	2,97%	58,56%

Risk Code	Risk	Risk Priority Number	Risk Level	Percentage of Total RPN	Accumulated Percentage
R4	The report submitted is less detailed	75	High	2,78%	61,34%
R7	The report accidentally submitted when it is not finished yet	75	High	2,78%	64,12%
R10	The fake/wrong report is verified	75	High	2,78%	66,90%
R18	The proposed date is not approved by the client	75	High	2,78%	69,68%
R24	There is a misperception toward the needs	75	High	2,78%	72,46%
R25	The client does not understand how the service run	75	High	2,78%	75,24%
R2	The user finds it hard to find "Laporkan Penipuan" button	60	Medium	2,22%	77,46%
R6	The user is not understood how to fill the form	60	Medium	2,22%	79,69%
R9	The report is submitted but not recorded in the database	60	Medium	2,22%	81,91%

Risk Code	Risk	Risk Priority Number	Risk Level	Percentage of Total RPN	Accumulated Percentage
R26	There is mistake inside the contract	60	Medium	2,22%	84,14%
R3	The user makes mistake in filling out the report form	50	Medium	1,85%	85,99%
R13	The client finds it hard to find "Enterprise" button	50	Medium	1,85%	87,84%
R8	The report cannot be submitted	40	Medium	1,48%	89,33%
R15	The client does not understand the description of the service	40	Medium	1,48%	90,81%
R27	Kredibel is failed to fulfill the agreed requirement	25	Medium	0,93%	91,73%
R31	The API key is given late	25	Medium	0,93%	92,66%
R32	The client does not understand how to insert API Key	25	Medium	0,93%	93,59%
R33	API Key cannot be used	25	Medium	0,93%	94,51%
R36	Billing cannot be used	25	Medium	0,93%	95,44%
R19	The email is forgotten to be sent	15	Low	0,56%	96,00%

Risk Code	Risk	Risk Priority Number	Risk Level	Percentage of Total RPN	Accumulated Percentage
R21	The email is sent but not arrive to the client	15	Low	0,56%	96,55%
R22	The email goes to spam folder	15	Low	0,56%	97,11%
R34	The API Key confirmation is not sent	15	Low	0,56%	97,66%
R35	The client does not understand how to refill billing	15	Low	0,56%	98,22%
R37	The billing confirmation is not sent	15	Low	0,56%	98,78%
R39	The client cannot understand the screening report	15	Low	0,56%	99,33%
R29	The terms & condition bring harm to Kredibel	10	Low	0,37%	99,70%
R38	The client makes mistake in inserting query	5	Low	0,19%	99,89%
R20	There is a mistake in email	3	Low	0,11%	100,00%
Total RPN (Risk Priority Number)		2698			

4.5.3 Operational Risk Priority Determination

The risk priority determination is done to define risks that needs more attention than other risks. The priority of the risks is determined using Pareto Law. Based on Pareto Law, 20% of cumulative RPN value will be the critical risks that is prioritized. The next following risks that have the same RPN value also included as the prioritized risks. Thus, prioritized risk consists of risks with RPN value of 125 or higher also the risks that have severity score of 5. Here is the list of prioritized operational risk in PT Kredibel Teknologi Indonesia based on Pareto.

Table 4.14 Kredibel Prioritized Risk

Risk Code	Risk
R1	The website cannot be accessed by user
R5	"Laporkan Penipuan" page cannot be accessed by user
R8	The report cannot be submitted
R11	The real/good report is not verified
R13	The client finds it hard to find "Enterprise" button
R14	The client failed to login
R23	The proposed requirement from the client cannot be fulfilled by Kredibel
R27	Kredibel is failed to fulfill the agreed requirement
R28	The terms & condition are not approved by the client
R29	The terms & condition bring harm to Kredibel
R30	There are some factors that is forgetten to consider
R31	The API key is given late
R32	The client does not understand how to insert API Key
R33	API Key cannot be used

Risk Code	Risk
R36	Billing cannot be used
R40	There is error in screening report
R41	There is no sufficient data/the data is less accurate
R42	The real/non-fraudster account classified as fake/fraudster account
R43	The fake/fraudster account classified as real/non-fraudster account

4.6 Operational Risk Treatment Alternative Scenario Determination

According to ISO 31000:2018, the next step is assigning several risk treatments to every operational risk in PT Kredibel Teknologi Indonesia. In this research, every risk has maximum two alternative treatments. After the treatments are assigned, three scenarios are conducted which will be compared in the next sub-chapter by using Benefit Cost Ratio to find the best scenario.

4.6.1 Operational Risk Treatment Alternative

Alternative treatments are assigned as a recommendation for the company to respond every risk. The mitigate treatments can be either avoid, reduce, transfer, or accept, and each reduce action is differentiated into three, which are to reduce the severity score, occurrence score, or detection score. In this research, one or two alternative treatments are assigned to every risk. The two alternative treatments can be either two reduce action or a reduce action and a "do nothing" action which is accept the risk. A risk treatment alternative scenario can be applied for more than one risk with similar risk category. Risks that are marked with bold lettering is risks that must be treated, which are included in extreme risks, high risks, or risks that have severity score of 5. The risks are grouped into website, fraud report, dealing process, and service way of use. Risks in the same category with different risk source may have the same risk treatment as long as the treatment can solve both the

risk sources. Here are alternatives of operational risk treatment in PT Kredibel Teknologi Indonesia.

Table 4.15 Kredibel Operational Risk Treatment Alternative

Risk Category		Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
				Type	To Reduce	Action	Type	To Reduce	Action
Website	Before using the service	User/Client	R2, R6, **R13**, R15	Mitigate	Occurrence	Conduct scheduled routine website maintenance including UI/UX optimization for Kredibel website.	Mitigate	Severity	Provide call center or customer care to respond complaints from users/clients about error on the website and questions from users/clients about how to use the website, so that the problem can be fixed immediately.
		System	**R1**, **R5**, **R8**, R12, **R14**,						
	While using the service	System	R34, R37						
		System	**R33**, **R36**,	Mitigate	Severity	Provide an employee	-	-	-

Risk Category		Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
				Type	To Reduce	Action	Type	To Reduce	Action
			R40			that responsible to be the technician for every client.			
Fraud Report	Form	User/Client	R3, **R4**, **R7**	Mitigate	Occurrence	Organize report form evaluation four times a year to standardize the report form and minimize mistakes in report	Mitigate	Severity	Allow user to edit reports after submitting them.

Risk Category		Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
				Type	To Reduce	Action	Type	To Reduce	Action
						submission (including adding additional feature such as confirmation checkbox or pop-up page before submitting the report).			
	Verification	Employee	**R10**, **R11**	Mitigate	Occurrence	Organize training twice a year for the workers that	-	-	-

Risk Category		Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
				Type	To Reduce	Action	Type	To Reduce	Action
						are responsible to verify the reports.			
	Database	System	R9	Mitigate	Occurrence	Allow user to monitor the submitted report and can resubmit the report if it is not submitted or complaint if the report is not processed	Accept	-	Do nothing.

Risk Category		Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
				Type	To Reduce	Action	Type	To Reduce	Action
						after several day.			
	Amount	System	**R41**	Mitigate	Occurrence	Use Instagram ads to raise awareness and influence people to report their fraud experience.	-	-	-
	Reliability	System	**R42**, **R43**	Mitigate	Severity	Allow user to give like or dislike for each report as additional	-	-	-

Risk Category		Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
				Type	To Reduce	Action	Type	To Reduce	Action
						reference. Likes toward a report are counted separately with how many it is being reported.			
Dealing Process	Needs	Employee	**R16**, **R17**, **R24**	Mitigate	Occurrence	Organize request form evaluation four times a year to standardize the request	Mitigate	Severity	Allow user to monitor the submitted needs and can edit them if it is not following the requirements.

Risk Category		Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
				Type	To Reduce	Action	Type	To Reduce	Action
						form and minimize mistakes in needs submission.			
	E-mail	Employee	R19, R20	Mitigate	Occurrence	Provide adequate performance management to prevent workers to make mistakes in sending email.	Accept	-	Do nothing.
		System	R21	Mitigate	Severity	Send a follow-up	Accept	-	Do nothing.

Risk Category		Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
				Type	To Reduce	Action	Type	To Reduce	Action
						email if the client does not respond in two days after the confirmation email sent.			
		System	R22	Mitigate	Severity	Add reminder on the website for client to always check their spam folder.	Accept	-	Do nothing.
	Appointment	Employee	**R18**	Mitigate	Occurrence	Add multiple input form	-	-	-

Risk Category		Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
				Type	To Reduce	Action	Type	To Reduce	Action
						of proposed appointment date while requesting the service.			
	Demo Day	User/Client	**R25**	Mitigate	Occurrence	Organize a regular evaluation twice a year for the service description, includes what can be fulfilled, how the	-	-	-

Risk Category		Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
				Type	To Reduce	Action	Type	To Reduce	Action
		Employee	**R23**, **R28**			service run, and the basic terms and condition based on the client's feedback.			
	Contract	Employee	R26, **R29**, **R30**	Mitigate	Occurrence	Organize a regular evaluation four times a year related	-	-	-

Risk Category		Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
				Type	To Reduce	Action	Type	To Reduce	Action
						to the SOP of non-disclosure agreement between Kredibel and the client.			
		Employee	**R27**, **R31**	Mitigate	Occurrence	Conduct different SOP related to service fulfillment for each client.	-	-	-
Service Way of Use		User/Client	**R32**, R35,	Mitigate	Severity	Provide an employee	-	-	-

Risk Category	Risk Source	Risk Code	Alternative Treatment 1			Alternative Treatment 2		
			Type	To Reduce	Action	Type	To Reduce	Action
		R38, R39			for clients that responsible to make sure that the client is able to use the service (customer support).			

4.6.2 Operational Risk Treatment Alternative Scenario

Six scenarios that consists of six different combination of risk treatment alternatives are conducted based on table above. These scenarios are conducted in order to find out which combination of risk treatment are the best to implement. Here are PT Kredibel Teknologi Indonesia Operational Risk Treatment Alternative Scenario.

Table 4.16 Operational Risk Treatment Alternative Scenario 1

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
Website	Before using the service	1	Mitigate	Occurrence	Conduct scheduled routine website maintenance including UI/UX optimization for Kredibel website.
	While using the service	1	Mitigate	Severity	Provide an employee that responsible to be the technician for every client.
Fraud Report	Form	1	Mitigate	Occurrence	Organize report form evaluation four times a year to standardize the report form and minimize mistakes in report submission (including adding additional feature such as confirmation checkbox or pop-up page before submitting the report).
	Verification	1	Mitigate	Occurrence	Organize training twice a year for the workers that are responsible to verify the reports.

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
	Database	1	Mitigate	Occurrence	Allow user to monitor the submitted report and can resubmit the report if it is not submitted or complaint if the report is not processed after several day.
	Amount	1	Mitigate	Occurrence	Use Instagram ads to raise awareness and influence people to report their fraud experience.
	Reliability	1	Mitigate	Severity	Allow user to give like or dislike for each report as additional reference. Likes toward a report are counted separately with how many it is being reported.
Dealing Process	Needs	1	Mitigate	Occurrence	Organize request form evaluation four times a year to standardize the request form and minimize mistakes in needs submission.

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
	E-mail	1	Mitigate	Occurrence	Provide adequate performance management to prevent workers to make mistakes in sending email.
		1	Mitigate	Severity	Send a follow-up email if the client does not respond in two days after the confirmation email sent.
		1	Mitigate	Severity	Add reminder on the website for client to always check their spam folder.
	Appointment	1	Mitigate	Occurrence	Add multiple input form of proposed appointment date while requesting the service.
	Demo Day	1	Mitigate	Occurrence	Organize a regular evaluation twice a year for the service description, includes what can be fulfilled, how the service run, and the basic terms and condition based on the client's feedback.
	Contract	1	Mitigate	Occurrence	Organize a regular evaluation four times a year related to the SOP of non-

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
					disclosure agreement between Kredibel and the client.
		1	Mitigate	Occurrence	Conduct different SOP related to service fulfillment for each client.
Service Way of Use		1	Mitigate	Severity	Provide an employee for clients that responsible to make sure that the client is able to use the service (customer support).

Table 4.17 Operational Risk Treatment Alternative Scenario 2

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
Website	Before using the service	2	Mitigate	Severity	Provide call center or customer care to respond complaints from users/clients about error on the website and questions from users/clients about how to use the website, so that the problem can be fixed immediately.
	While using the service				

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
		1	Mitigate	Severity	Provide an employee that responsible to be the technician for every client.
Fraud Report	Form	2	Mitigate	Severity	Allow user to edit reports after submitting them.
	Verification	1	Mitigate	Occurrence	Organize training twice a year for the workers that are responsible to verify the reports.
	Database	1	Mitigate	Occurrence	Allow user to monitor the submitted report and can resubmit the report if it is not submitted or complaint if the report is not processed after several day.
	Amount	1	Mitigate	Occurrence	Use Instagram ads to raise awareness and influence people to report their fraud experience.
	Reliability	1	Mitigate	Severity	Allow user to give like or dislike for each report as additional reference. Likes

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
					toward a report are counted separately with how many it is being reported.
Dealing Process	Needs	2	Mitigate	Severity	Allow user to monitor the submitted needs and can edit them if it is not following the requirements.
	E-mail	1	Mitigate	Occurrence	Provide adequate performance management to prevent workers to make mistakes in sending email.
		1	Mitigate	Severity	Send a follow-up email if the client does not respond in two days after the confirmation email sent.
		1	Mitigate	Severity	Add reminder on the website for client to always check their spam folder.
	Appointment	1	Mitigate	Occurrence	Add multiple input form of proposed appointment date while requesting the service.
	Demo Day	1	Mitigate	Occurrence	Organize a regular evaluation twice a year for the service description, includes

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
					what can be fulfilled, how the service run, and the basic terms and condition based on the client's feedback.
	Contract	1	Mitigate	Occurrence	Organize a regular evaluation four times a year related to the SOP of non-disclosure agreement between Kredibel and the client.
		1	Mitigate	Occurrence	Conduct different SOP related to service fulfillment for each client.
Service Way of Use		1	Mitigate	Severity	Provide an employee for clients that responsible to make sure that the client is able to use the service (customer support).

Table 4.18 Operational Risk Treatment Alternative Scenario 3

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
Website	Before using the service	1	Mitigate	Occurrence	Conduct scheduled routine website maintenance including UI/UX optimization for Kredibel website.
	While using the service	1	Mitigate	Severity	Provide an employee that responsible to be the technician for every client.
Fraud Report	Form	1	Mitigate	Occurrence	Organize report form evaluation four times a year to standardize the report form and minimize mistakes in report submission (including adding additional feature such as confirmation checkbox or pop-up page before submitting the report).
	Verification	1	Mitigate	Occurrence	Organize training twice a year for the workers that are responsible to verify the reports.

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
	Database	1	Mitigate	Occurrence	Allow user to monitor the submitted report and can resubmit the report if it is not submitted or complaint if the report is not processed after several day.
	Amount	1	Mitigate	Occurrence	Use Instagram ads to raise awareness and influence people to report their fraud experience.
	Reliability	1	Mitigate	Severity	Allow user to give like or dislike for each report as additional reference. Likes toward a report are counted separately with how many it is being reported.
Dealing Process	Needs	1	Mitigate	Occurrence	Organize request form evaluation four times a year to standardize the request form and minimize mistakes in needs submission.
	E-mail	2	Accept	-	Do nothing.
		2	Accept	-	Do nothing.

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
		2	Accept	-	Do nothing.
	Appointment	1	Mitigate	Occurrence	Add multiple input form of proposed appointment date while requesting the service.
	Demo Day	1	Mitigate	Occurrence	Organize a regular evaluation twice a year for the service description, includes what can be fulfilled, how the service run, and the basic terms and condition based on the client's feedback.
	Contract	1	Mitigate	Occurrence	Organize a regular evaluation four times a year related to the SOP of non-disclosure agreement between Kredibel and the client.
		1	Mitigate	Occurrence	Conduct different SOP related to service fulfillment for each client.
Service Way of Use		1	Mitigate	Severity	Provide an employee for clients that responsible to make sure that the client

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
					is able to use the service (customer support).

Table 4.19 Operational Risk Treatment Alternative Scenario 4

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
Website	Before using the service	1	Mitigate	Occurrence	Conduct scheduled routine website maintenance including UI/UX optimization for Kredibel website.
	While using the service	1	Mitigate	Severity	Provide an employee that responsible to be the technician for every client.
Fraud Report	Form	1	Mitigate	Occurrence	Organize report form evaluation four times a year to standardize the report form and minimize mistakes in report submission (including adding additional feature such as confirmation checkbox

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
					or pop-up page before submitting the report).
	Verification	1	Mitigate	Occurrence	Organize training twice a year for the workers that are responsible to verify the reports.
	Database	2	Accept	-	Do nothing.
	Amount	1	Mitigate	Occurrence	Use Instagram ads to raise awareness and influence people to report their fraud experience.
	Reliability	1	Mitigate	Severity	Allow user to give like or dislike for each report as additional reference. Likes toward a report are counted separately with how many it is being reported.
Dealing Process	Needs	1	Mitigate	Occurrence	Organize request form evaluation four times a year to standardize the request form and minimize mistakes in needs submission.

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
	E-mail	2	Accept	-	Do nothing.
		2	Accept	-	Do nothing.
		2	Accept	-	Do nothing.
	Appointment	1	Mitigate	Occurrence	Add multiple input form of proposed appointment date while requesting the service.
	Demo Day	1	Mitigate	Occurrence	Organize a regular evaluation twice a year for the service description, includes what can be fulfilled, how the service run, and the basic terms and condition based on the client's feedback.
	Contract	1	Mitigate	Occurrence	Organize a regular evaluation four times a year related to the SOP of non-disclosure agreement between Kredibel and the client.
		1	Mitigate	Occurrence	Conduct different SOP related to service fulfillment for each client.

Risk Category	Alternative Treatment	Treatment Type	To Reduce	Treatment Action
Service Way of Use	1	Mitigate	Severity	Provide an employee for clients that responsible to make sure that the client is able to use the service (customer support).

Table 4.20 Operational Risk Treatment Alternative Scenario 5

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
Website	Before using the service	2	Mitigate	Severity	Provide call center or customer care to respond complaints from users/clients about error on the website and questions from users/clients about how to use the website, so that the problem can be fixed immediately.
	While using the service	1	Mitigate	Severity	Provide an employee that responsible to be the technician for every client.

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
Fraud Report	Form	2	Mitigate	Severity	Allow user to edit reports after submitting them.
	Verification	1	Mitigate	Occurrence	Organize training twice a year for the workers that are responsible to verify the reports.
	Database	1	Mitigate	Occurrence	Allow user to monitor the submitted report and can resubmit the report if it is not submitted or complaint if the report is not processed after several day.
	Amount	1	Mitigate	Occurrence	Use Instagram ads to raise awareness and influence people to report their fraud experience.
	Reliability	1	Mitigate	Severity	Allow user to give like or dislike for each report as additional reference. Likes toward a report are counted separately with how many it is being reported.

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
Dealing Process	Needs	2	Mitigate	Severity	Allow user to monitor the submitted needs and can edit them if it is not following the requirements.
	E-mail	2	Accept	-	Do nothing.
		2	Accept	-	Do nothing.
		2	Accept	-	Do nothing.
	Appointment	1	Mitigate	Occurrence	Add multiple input form of proposed appointment date while requesting the service.
	Demo Day	1	Mitigate	Occurrence	Organize a regular evaluation twice a year for the service description, includes what can be fulfilled, how the service run, and the basic terms and condition based on the client's feedback.
	Contract	1	Mitigate	Occurrence	Organize a regular evaluation four times a year related to the SOP of non-disclosure agreement between Kredibel and the client.

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
		1	Mitigate	Occurrence	Conduct different SOP related to service fulfillment for each client.
Service Way of Use		1	Mitigate	Severity	Provide an employee for clients that responsible to make sure that the client is able to use the service (customer support).

Table 4.21 Operational Risk Treatment Alternative Scenario 6

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
Website	Before using the service	2	Mitigate	Severity	Provide call center or customer care to respond complaints from users/clients about error on the website and questions from users/clients about how to use the website, so that the problem can be fixed immediately.
	While using the service				

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
		1	Mitigate	Severity	Provide an employee that responsible to be the technician for every client.
Fraud Report	Form	2	Mitigate	Severity	Allow user to edit reports after submitting them.
	Verification	1	Mitigate	Occurrence	Organize training twice a year for the workers that are responsible to verify the reports.
	Database	2	Accept	-	Do nothing.
	Amount	1	Mitigate	Occurrence	Use Instagram ads to raise awareness and influence people to report their fraud experience.
	Reliability	1	Mitigate	Severity	Allow user to give like or dislike for each report as additional reference. Likes toward a report are counted separately with how many it is being reported.

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
Dealing Process	Needs	2	Mitigate	Severity	Allow user to monitor the submitted needs and can edit them if it is not following the requirements.
	E-mail	2	Accept	-	Do nothing.
		2	Accept	-	Do nothing.
		2	Accept	-	Do nothing.
	Appointment	1	Mitigate	Occurrence	Add multiple input form of proposed appointment date while requesting the service.
	Demo Day	1	Mitigate	Occurrence	Organize a regular evaluation twice a year for the service description, includes what can be fulfilled, how the service run, and the basic terms and condition based on the client's feedback.
	Contract	1	Mitigate	Occurrence	Organize a regular evaluation four times a year related to the SOP of non-disclosure agreement between Kredibel and the client.

Risk Category		Alternative Treatment	Treatment Type	To Reduce	Treatment Action
		1	Mitigate	Occurrence	Conduct different SOP related to service fulfillment for each client.
Service Way of Use		1	Mitigate	Severity	Provide an employee for clients that responsible to make sure that the client is able to use the service (customer support).

4.7 Operational Risk Treatment Alternative Scenario Assessment

The assessment of operational risk treatment alternative scenario is a continuation of the previous step. This assessment is done to determine which risk treatment is the best to be implemented with benefit and cost as the indicator. Thus, benefit cost ratio is used in this assessment. Every benefit and cost components have proxy to explain how big the benefit and the cost of every risk treatment. The proxy is only based on the company's preference. Both component and proxy will be reviewed and approved by the company.

4.7.1 Operational Risk Treatment Benefit Component Identification

Benefit component identification is done to measure how much benefit in term of profit or cost savings if a treatment is done for a risk. Benefit components that being identified are benefit that obtained directly or the main benefit if a risk is being treated. The benefit components are differentiated into two which are when the treatment has an aim to reduce the severity score of the risk and to reduce the occurrence score of the risk. The benefit that is calculated per component refers to benefit that the company obtains if a risk

treatment action is done. For example, if the company applied two risk treatment actions that have the same benefit component, the benefit that the company get is a double of the component. Here is the result of operational risk treatment benefit component identification in PT Kredibel Teknologi Indonesia.

Table 4.22 Operational Risk Treatment Benefit Component (Severity)

Reduce Action	Type	Benefit						
		Lengthen duration client uses the service	Raise number of clients	Reduce cost spent to fix the website	Shorten Duration of Verification Process	Shorten Contract Agreement Process	Reduce number of clients that cancel the usage of service during dealing process	Eliminate fine to clients
Provide call center or customer care to respond complaints from users/clients about error on the website and questions from users/clients about how to use the website, so that the problem can be fixed immediately.	Curative	✓	✓					

Reduce Action	Type	Benefit						
		Lengthen duration client uses the service	Raise number of clients	Reduce cost spent to fix the website	Shorten Duration of Verification Process	Shorten Contract Agreement Process	Reduce number of clients that cancel the usage of service during dealing process	Eliminate fine to clients
Provide an employee that responsible to be the technician for every client.	Curative	✓						
Allow user to edit reports after submitting them.	Preventive	✓						
Allow user to give like or dislike for each report as additional reference. Likes toward a report	Preventive		✓					

Reduce Action	Type	Benefit						
		Lengthen duration client uses the service	Raise number of clients	Reduce cost spent to fix the website	Shorten Duration of Verification Process	Shorten Contract Agreement Process	Reduce number of clients that cancel the usage of service during dealing process	Eliminate fine to clients
are counted separately with how many it is being reported.								
Allow user to monitor the submitted needs and can edit them if it is not following the requirements.	Curative					✓		
Send a follow-up email if the client does not respond in two days after the	Curative						✓	

Reduce Action	Type	Benefit						
		Lengthen duration client uses the service	Raise number of clients	Reduce cost spent to fix the website	Shorten Duration of Verification Process	Shorten Contract Agreement Process	Reduce number of clients that cancel the usage of service during dealing process	Eliminate fine to clients
confirmation email sent.								
Add reminder on the website for client to always check their spam folder.	Preventive						✓	
Provide an employee for clients that responsible to make sure that the client is able to use the service (customer support).	Preventive	✓						

Table 4.23 Operational Risk Treatment Benefit Component (Occurrence)

Reduce Action	Type	Benefit						
		Lengthen duration client uses the service	Raise number of clients	Reduce cost spent to fix the website	Shorten Duration of Verification Process	Shorten Contract Agreement Process	Reduce number of clients that cancel the usage of service during dealing process	Eliminate fine to clients
Conduct scheduled routine website maintenance including UI/UX optimization for Kredibel website.	Preventive	✓	✓	✓				
Organize report form evaluation four times a year to standardize the report form and minimize mistakes in report submission	Preventive	✓			✓			

Reduce Action	Type	Benefit						
		Lengthen duration client uses the service	Raise number of clients	Reduce cost spent to fix the website	Shorten Duration of Verification Process	Shorten Contract Agreement Process	Reduce number of clients that cancel the usage of service during dealing process	Eliminate fine to clients
(including adding additional feature such as confirmation checkbox or pop-up page before submitting the report).								
Organize training twice a year for the workers that are responsible to verify the reports.	Preventive	✓						

Reduce Action	Type	Benefit						
		Lengthen duration client uses the service	Raise number of clients	Reduce cost spent to fix the website	Shorten Duration of Verification Process	Shorten Contract Agreement Process	Reduce number of clients that cancel the usage of service during dealing process	Eliminate fine to clients
Allow user to monitor the submitted report and can resubmit the report if it is not submitted or complaint if the report is not processed after several day.	Curative	✓						
Use Instagram ads to raise awareness and influence people to report their fraud experience.	Preventive		✓					

Reduce Action	Type	Benefit						
		Lengthen duration client uses the service	Raise number of clients	Reduce cost spent to fix the website	Shorten Duration of Verification Process	Shorten Contract Agreement Process	Reduce number of clients that cancel the usage of service during dealing process	Eliminate fine to clients
Organize request form evaluation four times a year to standardize the request form and minimize mistakes in needs submission.	Preventive					✓		
Provide adequate performance management to prevent workers to make mistakes in sending email.	Preventive					✓		

Reduce Action	Type	Benefit						
		Lengthen duration client uses the service	Raise number of clients	Reduce cost spent to fix the website	Shorten Duration of Verification Process	Shorten Contract Agreement Process	Reduce number of clients that cancel the usage of service during dealing process	Eliminate fine to clients
Add multiple input form of proposed appointment date while requesting the service.	Preventive					✓		
Organize a regular evaluation twice a year for the service description, includes what can be fulfilled, how the service run, and the basic terms and condition based	Preventive						✓	

Reduce Action	Type	Benefit						
		Lengthen duration client uses the service	Raise number of clients	Reduce cost spent to fix the website	Shorten Duration of Verification Process	Shorten Contract Agreement Process	Reduce number of clients that cancel the usage of service during dealing process	Eliminate fine to clients
on the client's feedback.								
Organize a regular evaluation four times a year related to the SOP of non-disclosure agreement between Kredibel and the client.	Preventive						✓	
Conduct different SOP related to service	Preventive	✓						✓

Reduce Action	Type	Benefit						
		Lengthen duration client uses the service	Raise number of clients	Reduce cost spent to fix the website	Shorten Duration of Verification Process	Shorten Contract Agreement Process	Reduce number of clients that cancel the usage of service during dealing process	Eliminate fine to clients
fulfillment for each client.								

Table 4.24 Operational Risk Treatment Benefit Proxy

Component	Proxy	Total in 1 Year
Lengthen duration client uses the service (at least 1 month extension)	Average monthly income per client x the highest number of clients in a year x additional duration of client uses the service	Rp 9,000,000
Raise number of clients (at least 1 client addition)	Average monthly income per client x additional number of clients x the shortest duration client uses the service	Rp 6,000,000

Component	Proxy	Total in 1 Year
Reduce cost spent to fix the website	Daily website engineer's wage x duration of website repairment in days x how many times the website has problem in a year	Rp 1,454,545.45
Shorten duration of verification process	Number of reports that have to be verified in a year x reduced verification duration / 60 minutes x verification fee per hour	Rp 3,555,555.56
Shorten contract agreement process (at least 1 month duration reduction)	Average monthly income per client x the highest number of clients in a year x reduction of contract agreement process duration	Rp 9,000,000
Reduce number of clients that cancel the usage of service during dealing process (at least 1 client reduction)	Average monthly income per client x reduction of number of clients that cancel the usage of service x the shortest duration client uses the service in months	Rp 6,000,000
Eliminate fine	Maximum possible fine per client based on NDA x the highest number of clients in a year	Rp 9,000,000

4.7.2 Operational Risk Treatment Cost Component Identification

Cost component identification is done to measure how much cost that being used for every risk treatment that are already identified in previous sub-chapter. The cost treatment is differentiated into two, which are Capital Expenditure (CAPEX) and Operational Expenditure (OPEX). Here is the result of operational risk treatment cost component identification in PT Kredibel Teknologi Indonesia.

Table 4.25 Operational Risk Treatment Cost Component and Proxy (Severity)

Treatment Action	Cost	Capital Expenditure (CAPEX)			Operational Expenditure (OPEX)		
		Component	Proxy	Total in 1 Year	Component	Proxy	Total in 1 Year
Provide call center or customer care to respond complaints from users/clients about error on the website and questions from users/clients about how to use the website, so that the	Hire one admin intern	Recruitment Cost	2 x daily recruitment staff's wage x 5 days	Rp 3,636,363.64	Admin's wage (intern)	Monthly intern's wage x 12 months	Rp 12,000,000

Treatment Action	Cost	Capital Expenditure (CAPEX)			Operational Expenditure (OPEX)		
		Component	Proxy	Total in 1 Year	Component	Proxy	Total in 1 Year
problem can be fixed immediately.							
Provide an employee that responsible to be the technician for every client.	Hire three technician interns	Recruitment Cost	2 x daily recruitment staff's wage x 5 days	Rp 3,636,363.64	Technician's wage (Intern)	Monthly new worker's wage x 12 months x the highest number of clients in a year	Rp 36,000,000
Allow user to edit reports after submitting them.	Additional feature on the website	Involved worker's wage	Daily website engineer's wage x 5 days	Rp1,818,181.82	-	-	-

Treatment Action	Cost	Capital Expenditure (CAPEX)			Operational Expenditure (OPEX)		
		Component	Proxy	Total in 1 Year	Component	Proxy	Total in 1 Year
Allow user to give like or dislike for each report as additional reference. Likes toward a report are counted separately with how many it is being reported.	Additional feature on the website	Involved worker's wage	Daily website engineer's wage x 5 days	Rp1,818,181.82	-	-	-
Allow user to monitor the submitted needs and can edit them if it is not following the requirements.	Additional feature on the website	Involved worker's wage	Daily website engineer's wage x 5 days	Rp1,818,181.82	-	-	-

Treatment Action	Cost	Capital Expenditure (CAPEX)			Operational Expenditure (OPEX)		
		Component	Proxy	Total in 1 Year	Component	Proxy	Total in 1 Year
Send a follow-up email if the client does not respond in two days after the confirmation email sent.	Email making and sending	-	-	-	Involved worker's wage	Daily worker's wage x 1 day	Rp 363,636.36
Add reminder on the website for client to always check their spam folder.	Additional information on the website	Involved worker's wage	Daily worker's wage x 1 day x the highest	Rp363,636.36	-	-	-
Provide an employee for clients that responsible to make sure that the client is able to use	Hire one new intern	Recruitment Cost	2 x daily recruitment staff's wage x 5 days	Rp 3,636,363.64	Worker's wage (intern)	Monthly intern's wage x 12 months	Rp 12,000,000

Treatment Action	Cost	Capital Expenditure (CAPEX)			Operational Expenditure (OPEX)		
		Component	Proxy	Total in 1 Year	Component	Proxy	Total in 1 Year
the service (customer support).							

Table 4.26 Operational Risk Treatment Cost Component (Occurrence)

Treatment Action	Cost	Capital Expenditure (CAPEX)			Operational Expenditure (OPEX)		
		Component	Proxy	Total in 1 Year	Component	Proxy	Total in 1 Year
Conduct scheduled routine website maintenance including UI/UX optimization for Kredibel website.	Website maintenance	-	-	-	Website maintenance cost	Monthly website maintenance cost x 12 months	Rp 27,000,000
Organize report form evaluation four times a year to standardize the	Report form evaluation	-	-	-	Involved worker's wage (1 back-end	Daily worker's wage x 4 days	Rp 3,818,181.82

Treatment Action	Cost	Capital Expenditure (CAPEX)			Operational Expenditure (OPEX)		
		Component	Proxy	Total in 1 Year	Component	Proxy	Total in 1 Year
report form and minimize mistakes in report submission (including adding additional feature such as confirmation checkbox or pop-up page before submitting the report).					staff, 1 front-end staff, 1 intern)		
Organize training twice a year for the workers that are responsible to verify the reports.	Verifier training	-	-	-	Training cost	Training cost x 2	Rp 1,000,000

Treatment Action	Cost	Capital Expenditure (CAPEX)			Operational Expenditure (OPEX)		
		Component	Proxy	Total in 1 Year	Component	Proxy	Total in 1 Year
Allow user to monitor the submitted report and can resubmit the report if it is not submitted or complaint if the report is not processed after several day.	Additional feature on the website	Involved worker's wage	Daily website engineer's wage x 5 days	Rp1,818,181.82	-	-	-
Use Instagram ads to raise awareness and influence people to report their fraud experience.	Instagram ads	-	-	-	Instagram ads cost	Monthly Instagram ads x 12 months	Rp 427,614

Treatment Action	Cost	Capital Expenditure (CAPEX)			Operational Expenditure (OPEX)		
		Component	Proxy	Total in 1 Year	Component	Proxy	Total in 1 Year
Organize request form evaluation four times a year to standardize the request form and minimize mistakes in needs submission.	Request form evaluation	-	-	-	Involved worker's wage (B2B service and website engineer)	Daily worker's wage x 4 days	Rp 7,090,909.09
Provide adequate performance management to prevent workers to make mistakes in sending email.	Improve performance management	-	-	-	Performance management cost	Number of employee x performance cost per employee per month x 12 months	Rp 4,320,000

Treatment Action	Cost	Capital Expenditure (CAPEX)			Operational Expenditure (OPEX)		
		Component	Proxy	Total in 1 Year	Component	Proxy	Total in 1 Year
Add multiple input form of proposed appointment date while requesting the service.	Additional feature on the website	Involved worker's wage	Daily website engineer's wage x 5 days	Rp1,818,181.82	-	-	-
Organize a regular evaluation twice a year for the service description, includes what can be fulfilled, how the service run, and the basic terms and condition based on the client's feedback.	Service description evaluation	-	-	-	Involved worker's wage (B2B service)	Daily worker's wage x 2 days	Rp1,727,272.73

Treatment Action	Cost	Capital Expenditure (CAPEX)			Operational Expenditure (OPEX)		
		Component	Proxy	Total in 1 Year	Component	Proxy	Total in 1 Year
Organize a regular evaluation four times a year related to the SOP of non-disclosure agreement between Kredibel and the client.	NDA making evaluation	-	-	-	Involved worker's wage (B2B service and legal staff)	Daily worker's wage x 4 days	Rp 5,090,909.09
Conduct different SOP related to service fulfillment for each client.	SOP making for every client	-	-	-	Involved worker's wage (B2B service)	Daily worker's wage x 1 day x the highest number of clients in a year	Rp 2,590,909.09

4.7.3 Operational Risk Treatment Benefit Cost Ratio Calculation

Benefit cost ratio calculation is using the components from sub-sub-chapter 4.7.1 and 4.7.2. All benefit and cost components have each proxy that is defined by the author and approved by the company. Benefit cost ratio is calculated by using **Formula (2-4)** in **Sub-chapter 2.7**. The benefit cost ratio is involved by benefit and cost that happened during 2021 and 2022. Here is the result of operational risk treatment benefit cost ratio calculation in PT Kredibel Teknologi Indonesia.

Table 4.27 Benefit Calculation of Scenario 1

Benefit	Present Value	
	2021	2022
Lengthen duration client uses the service	Rp 63.000.000,00	Rp 63.000.000,00
Raise Number of clients	Rp 18.000.000,00	Rp 18.000.000,00
Reduce cost spent to fix the website	Rp 1.454.545,45	Rp 1.454.545,45
Shorten duration of verification process	Rp 3.555.555,56	Rp 3.555.555,56
Shorten contract agreement process	Rp 27.000.000,00	Rp 27.000.000,00
Reduce number of clients that cancel the usage of service during dealing process	Rp 24.000.000,00	Rp 24.000.000,00
Eliminate fines to clients	Rp 9.000.000,00	Rp 9.000.000,00
Total	Rp 146.010.010,01	Rp 146.010.101,01
Benefit of Scenario 1	**Rp 292.020.202,02**	

Table 4.28 Benefit Calculation of Scenario 2

Benefit	Present Value	
	2021	2022
Lengthen duration client uses the service	Rp 63.000.000,00	Rp 63.000.000,00
Raise Number of clients	Rp 18.000.000,00	Rp 18.000.000,00
Shorten contract agreement process	Rp 27.000.000,00	Rp 27.000.000,00
Reduce number of clients that cancel the usage of service during dealing process	Rp 24.000.000,00	Rp 24.000.000,00
Eliminate fines to clients	Rp 9.000.000,00	Rp 9.000.000,00
Total	Rp 141.000.000,00	Rp 141.000.000,00
Benefit of Scenario 2	**Rp 282.000.000,00**	

Table 4.29 Benefit Calculation of Scenario 3

Benefit	Present Value	
	2021	2022
Lengthen duration client uses the service	Rp 63.000.000,00	Rp 63.000.000,00
Raise Number of clients	Rp 18.000.000,00	Rp 18.000.000,00
Reduce cost spent to fix the website	Rp 1.454.545,45	Rp 1.454.545,45
Shorten duration of verification process	Rp 3.555.555,56	Rp 3.555.555,56
Shorten contract agreement process	Rp 18.000.000,00	Rp 18.000.000,00
Reduce number of clients that cancel the usage of service during dealing process	Rp 12.000.000,00	Rp 12.000.000,00
Eliminate fines to clients	Rp 9.000.000,00	Rp 9.000.000,00

Benefit	Present Value	
	2021	2022
Total	Rp 125.010.010,01	Rp 125.010.101,01
Benefit of Scenario 3	**Rp 250.020.202,02**	

Table 4.30 Benefit Calculation of Scenario 4

Benefit	Present Value	
	2021	2022
Lengthen duration client uses the service	Rp 54.000.000,00	Rp 54.000.000,00
Raise Number of clients	Rp 18.000.000,00	Rp 18.000.000,00
Reduce cost spent to fix the website	Rp 1.454.545,45	Rp 1.454.545,45
Shorten duration of verification process	Rp 3.555.555,56	Rp 3.555.555,56
Shorten contract agreement process	Rp 18.000.000,00	Rp 18.000.000,00
Reduce number of clients that cancel the usage of service during dealing process	Rp 12.000.000,00	Rp 12.000.000,00
Eliminate fines to clients	Rp 9.000.000,00	Rp 9.000.000,00
Total	Rp 126.010.010,01	Rp 126.010.101,01
Benefit of Scenario 4	**Rp 232.020.202,02**	

Table 4.31 Benefit Calculation of Scenario 5

Benefit	Present Value	
	2021	2022
Lengthen duration client uses the service	Rp 63.000.000,00	Rp 63.000.000,00
Raise Number of clients	Rp 18.000.000,00	Rp 18.000.000,00

Benefit	Present Value	
	2021	2022
Shorten contract agreement process	Rp 18.000.000,00	Rp 18.000.000,00
Reduce number of clients that cancel the usage of service during dealing process	Rp 12.000.000,00	Rp 12.000.000,00
Eliminate fines to clients	Rp 9.000.000,00	Rp 9.000.000,00
Total	Rp 120.000.000,00	Rp 120.000.000,00
Benefit of Scenario 5	**Rp 240.000.000,00**	

Table 4.32 Benefit Calculation of Scenario 6

Benefit	Present Value	
	2021	2022
Lengthen duration client uses the service	Rp 54.000.000,00	Rp 54.000.000,00
Raise Number of clients	Rp 18.000.000,00	Rp 18.000.000,00
Shorten contract agreement process	Rp 18.000.000,00	Rp 18.000.000,00
Reduce number of clients that cancel the usage of service during dealing process	Rp 12.000.000,00	Rp 12.000.000,00
Eliminate fines to clients	Rp 9.000.000,00	Rp 9.000.000,00
Total	Rp 111.000.000,00	Rp 111.000.000,00
Benefit of Scenario 6	**Rp 222.000.000,00**	

Table 4.33 Cost Calculation of Scenario 1

Cost	Present Value	
	2021	2022
Website maintenance	Rp 27.000.000,00	Rp 27.000.000,00
Hire three technician interns	Rp 42.336.363,64	Rp 36.000.000,00

Cost	Present Value	
	2021	2022
Report form evaluation	Rp 3.818.181,82	Rp 3.818.181,82
Training for verifier	Rp 1.000.000,00	Rp 1.000.000,00
Additional feature on the website	Rp 5.454.545,46	-
Instagram ads	Rp 427.614,00	Rp 427.614,00
Request form evaluation	Rp 7.090.909,09	Rp 7.090.909,09
Improve performance management	Rp 4.320.000,00	Rp 4.320.000,00
Email making and sending	Rp 363.636,36	Rp 363.636,36
Additional information on the website	Rp 363.636,36	-
Service description evaluation	Rp 1.727.272,73	Rp 1.727.272,73
NDA making evaluation	Rp 5.090.909,09	Rp 5.090.909,09
SOP making for every client	Rp 2.590.909,09	Rp 2.590.909,09
Hire one new worker	Rp 15.636.363,64	Rp 12.000.000,00
Total	Rp 117.220.341,28	Rp 101.429.432,18
Cost of Scenario 1	**Rp 218.649.773,46**	

Table 4.34 Cost Calculation of Scenario 2

Cost	Present Value	
	2021	2022
Hire one admin	Rp 15.636.363,64	Rp 12.000.000,00
Hire three technician interns	Rp 42.336.363,64	Rp 36.000.000,00
Additional feature on the website	Rp 9.090.909,9	-
Training for verifier	Rp 1.000.000,00	Rp 1.000.000,00
Instagram ads	Rp 427.614,00	Rp 427.614,00
Improve performance management	Rp 4.320.000,00	Rp 4.320.000,00

Cost	Present Value	
	2021	2022
Email making and sending	Rp 363.636,36	Rp 363.636,36
Additional information on the website	Rp 363.636,36	-
Service description evaluation	Rp 1.727.272,73	Rp 1.727.272,73
NDA making evaluation	Rp 5.090.909,09	Rp 5.090.909,09
SOP making for every client	Rp 2.590.909,09	Rp 2.590.909,09
Hire one new worker	Rp 15.636.363,64	Rp 12.000.000,00
Total	Rp 98.583.978,65	Rp 75.520.341,27
Cost of Scenario 2	**Rp 174.104.319,92**	

Table 4.35 Cost Calculation of Scenario 3

Cost	Present Value	
	2021	2022
Website maintenance	Rp 27.000.000,00	Rp 27.000.000,00
Hire three technician interns	Rp 42.336.363,64	Rp 36.000.000,00
Report form evaluation	Rp 3.818.181,82	Rp 3.818.181,82
Training for verifier	Rp 1.000.000,00	Rp 1.000.000,00
Additional feature on the website	Rp 5.454.545,46	-
Instagram ads	Rp 427.614,00	Rp 427.614,00
Request form evaluation	Rp 7.090.909,09	Rp 7.090.909,09
Service description evaluation	Rp 1.727.272,73	Rp 1.727.272,73
NDA making evaluation	Rp 5.090.909,09	Rp 5.090.909,09
SOP making for every client	Rp 2.590.909,09	Rp 2.590.909,09
Hire one new worker	Rp 15.636.363,64	Rp 12.000.000,00
Total	Rp 112.173.068,56	Rp 96.745.795,82
Cost of Scenario 3	**Rp 208.918.864,38**	

Table 4.36 Cost Calculation of Scenario 4

Cost	Present Value	
	2021	2022
Website maintenance	Rp 27.000.000,00	Rp 27.000.000,00
Hire three technician interns	Rp 42.336.363,64	Rp 36.000.000,00
Report form evaluation	Rp 3.818.181,82	Rp 3.818.181,82
Training for verifier	Rp 1.000.000,00	Rp 1.000.000,00
Additional feature on the website	Rp 3.636.363,64	-
Instagram ads	Rp 427.614,00	Rp 427.614,00
Request form evaluation	Rp 7.090.909,09	Rp 7.090.909,09
Service description evaluation	Rp 1.727.272,73	Rp 1.727.272,73
NDA making evaluation	Rp 5.090.909,09	Rp 5.090.909,09
SOP making for every client	Rp 2.590.909,09	Rp 2.590.909,09
Hire one new worker	Rp 15.636.363,64	Rp 12.000.000,00
Total	Rp 110.354.886,74	Rp 96.745.795,82
Cost of Scenario 4	**Rp 207.100.682,56**	

Table 4.37 Cost Calculation of Scenario 5

Cost	Present Value	
	2021	2022
Hire one admin	Rp 15.636.363,64	Rp 12.000.000,00
Hire three technician interns	Rp 42.336.363,64	Rp 36.000.000,00
Additional feature on the website	Rp 9.090.909,9	-
Training for verifier	Rp 1.000.000,00	Rp 1.000.000,00
Instagram ads	Rp 427.614,00	Rp 427.614,00
Service description evaluation	Rp 1.727.272,73	Rp 1.727.272,73
NDA making evaluation	Rp 5.090.909,09	Rp 5.090.909,09
SOP making for every client	Rp 2.590.909,09	Rp 2.590.909,09
Hire one new worker	Rp 15.636.363,64	Rp 12.000.000,00

Cost	Present Value	
	2021	2022
Total	Rp 93.536.705,93	Rp 70.836.704,91
Cost of Scenario 5	**Rp 164.373.410,84**	

Table 4.38 Cost Calculation of Scenario 6

Cost	Present Value	
	2021	2022
Hire one admin	Rp 15.636.363,64	Rp 12.000.000,00
Hire three technician interns	Rp 42.336.363,64	Rp 36.000.000,00
Additional feature on the website	Rp 7.272.727,28	-
Training for verifier	Rp 1.000.000,00	Rp 1.000.000,00
Instagram ads	Rp 427.614,00	Rp 427.614,00
Service description evaluation	Rp 1.727.272,73	Rp 1.727.272,73
NDA making evaluation	Rp 5.090.909,09	Rp 5.090.909,09
SOP making for every client	Rp 2.590.909,09	Rp 2.590.909,09
Hire one new worker	Rp 15.636.363,64	Rp 12.000.000,00
Total	Rp 91.718.523,11	Rp 70.836.704,91
Cost of Scenario 6	**Rp 162.555.228,02**	

Table 4.39 The Result of Benefit Cost Ratio Calculation (Ascendant Benefit)

Alternative	Total Present Value		Benefit Cost Ratio
	Benefit	Cost	
Scenario 1	Rp292,020,202.02	Rp218,649,773.46	1.34
Scenario 2	Rp282,000,000.00	Rp174,104,319.92	1.62
Scenario 3	Rp250,020,202.02	Rp208,918,864.38	1.20
Scenario 5	Rp240,000,000.00	Rp164,373,410.84	1.46
Scenario 4	Rp232,020,202.02	Rp207,100,682.56	1.12
Scenario 6	Rp222,000,000.00	Rp162,555,228.02	1.37

The benefit cost ratio value is >1 for every scenario. It means that all the scenarios are feasible to be implemented. To choose the most preferable alternative scenario, incremental benefit scenario is used. Here is the result of incremental benefit cost ratio calculation.

Table 4.40 The Result of Incremental Benefit Cost Ratio Calculation

Alternative	ΔBenefit	ΔCost	Ratio (ΔBenefit/ ΔCost)	Decision
Scenario 6 – 0	Rp222,000,000,00	Rp162,555,228.02	1.37	Accept Scenario 6
Scenario 4 – Scenario 6	Rp10,020,202.02	Rp44,545,453.54	0.22	Reject Scenario 4
Scenario 5 – Scenario 6	Rp18,000,000.00	Rp1,818,182.82	9.90	Accept Scenario 5
Scenario 3 – Scenario 5	Rp10,020,202.02	Rp44,545,453.54	0.22	Reject Scenario 3
Scenario 2 – Scenario 5	Rp42,000,000.00	Rp9,730,909.08	4.32	Accept Scenario 2
Scenario 1 – Scenario 2	Rp10,020,202.02	Rp44,545,453.54	0.22	Reject Scenario 1

It can be seen in the result of incremental benefit cost ratio that Scenario 2 is the most preferable scenario among all the scenarios.

CHAPTER 5
DATA ANALYSIS AND INTERPRETATION

In this chapter, there will be explanation about the analysis and interpretation of the data processing result from chapter 4. The context of this chapter depends on the objectives that already stated in the beginning of this research.

5.1 Analysis of Operational Risk Identification

In this research, the risk management is implemented by using ISO 31000:2018 and specifically for a B2B service called Fraud Management System with pre-paid payment. Based on ISO 31000:2018, the risk assessment consists of risk identification, risk analysis, and risk evaluation. The risk identification is done based on the activities that are broken-down using a framework called service blueprint. Three blueprints are made based on the process, which are data gathering process, contract agreement process, and service fulfillment process. Data gathering process consists of activities related to the making of the fraud database. Contract agreement process contains activities during the dealing process between Kredibel and the client. While service fulfillment process contains activities that happens after the contract made and the client is start using the service. In service blueprint, there are several types of components. Only customer action, onstage action, and backstage action components that are used as activities in risk identification because those activities are directly related with the company and any mistake and error related to those activities may give significant impact to the company. There are six activities in data gathering process, eleven activities in contract agreement process, and seven activities in service fulfillment process that are identified by using service blueprint. The risks of each activity are being identified in the risk identification process. Beside based on the activities, the risks are also identified based on the source of the risks, which are user/client, employee, and system. It is done to make sure that there is no risk missed to be identified. After the list of risks are being made, those risks are being validated to the representative of the company that highly related with the service and considered as expert which is the Head of

Business. The risks are being identified based on direct interview to the company and document interpretation, which are Service Operational Procedur (SOP), Non-Disclosure Agreement (NDA) draft, and other document related to the risk management that is already implemented in Kredibel. The identified risks are events that may give financial loss to the company. 43 operational risks of PT Kredibel Teknologi Indonesia are being identified and validated in the risk identification process.

5.2 Analysis of Operational Risk Analysis and Evaluation

Based on ISO 31000:2018, the next step will be risk analysis and risk evaluation. The risk impact, cause and control are assigned to every identified risk based on direct interview and document interpretation as well. These factors are used to score the severity, occurrence, and detection of the risks. Since Kredibel is a startup company, it only consists of several workers, and they have their own job. Thus, the one that fully understand about Fraud Management System is the Head of Business. The score filling is done by direct interview to the Head of Business to make sure that the respondent is understanding every risk. To maintain the accuracy of the score, the director of the company must review and approve them. There are three score dimensions, which are severity, occurrence, and detection. The severity, occurrence, and detection score are given based on the rating indicator that is already validated by the company. Every dimension is scored in a scale of 1 to 5. Here are the visualization of severity, occurrence, and detection score of the risks.

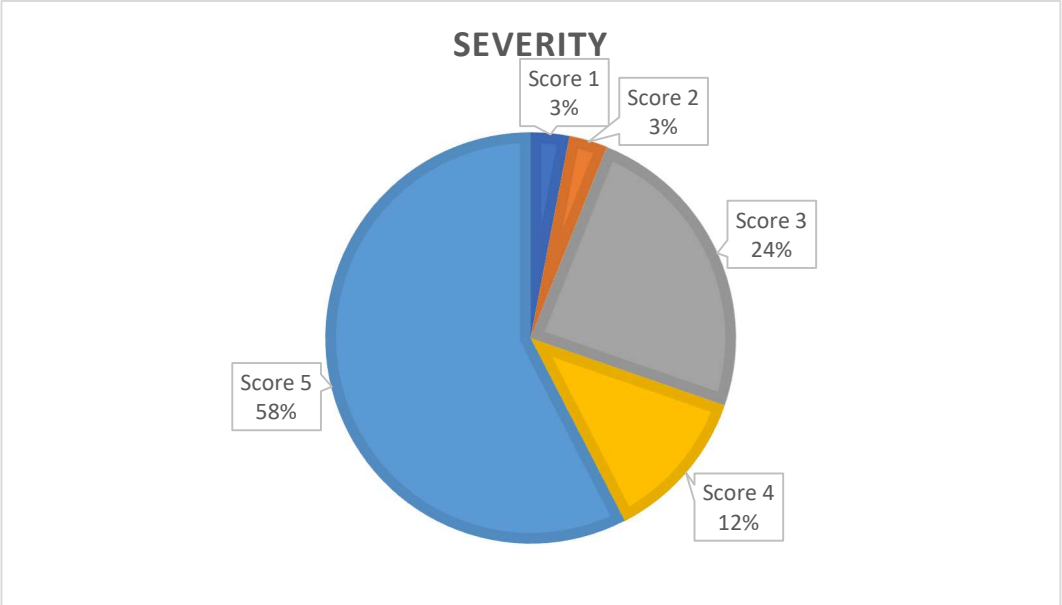

Figure 5.1 Severity Score Proportion

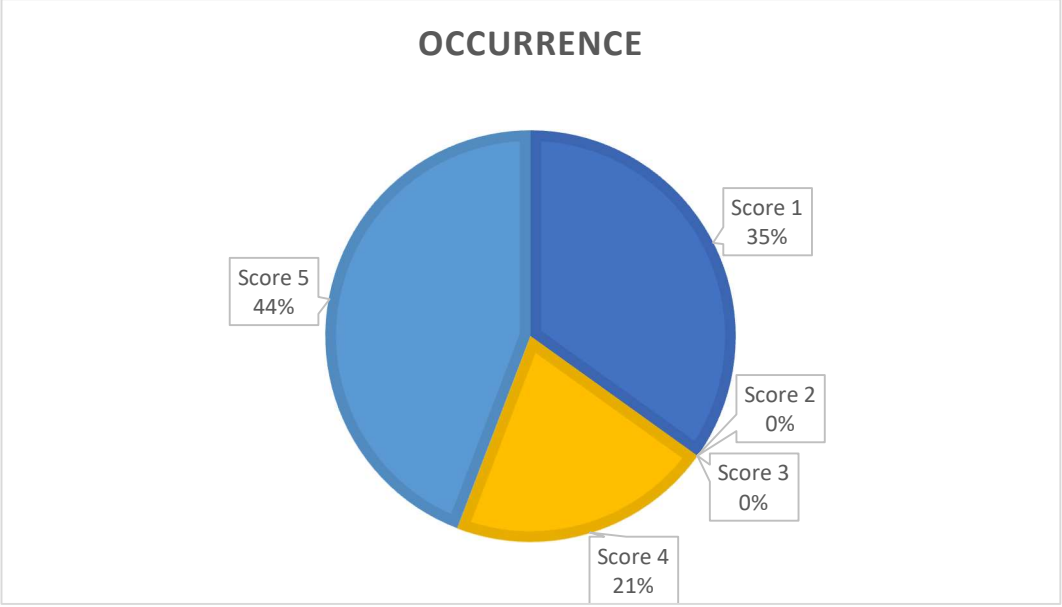

Figure 5.2 Occurrence Score Proportion

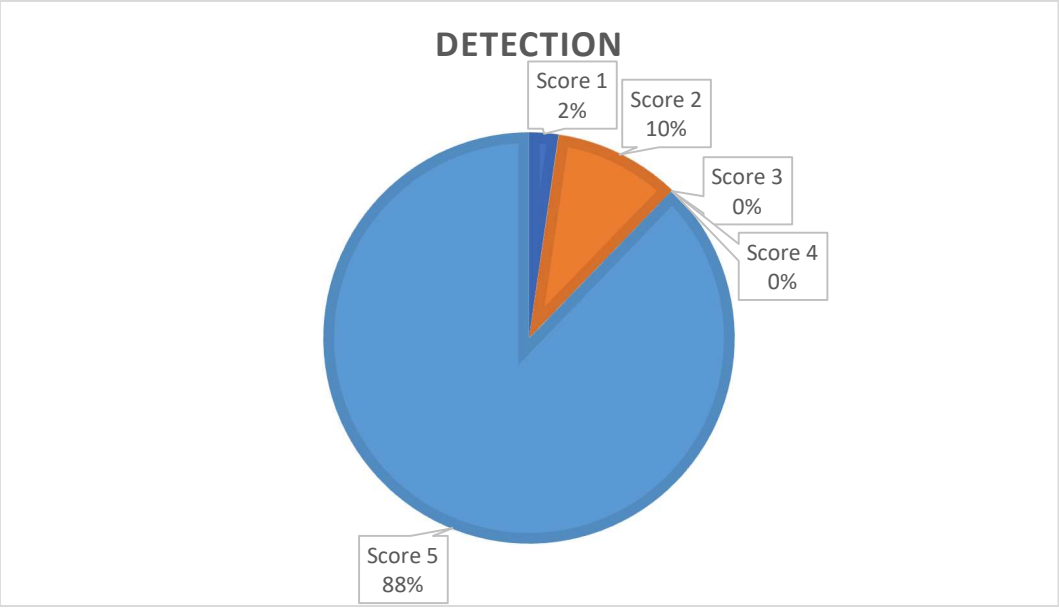

Figure 5.3 Detection Score Proportion

Then, Risk Priority Number (RPN) is calculated. RPN value is the multiplication of severity score, occurrence score, and detection score. The lowest possible RPN value is 1 and the highest is 125. Based on the RPN calculation, the highest RPN value is 125, which is owned by 8 risks. It means that those risks have significant impact that can stop the whole activities, occur very recently which is in the last three months, and has no possibility to be detected. The lowest RPN value is 3, which is owned by the risk of there is mistake in email. It means that it only has impact to several processes, never occurs before, and almost certainly to be detected. Based on RPN, the level of each risk is identified. Risk level is differentiated into four which are extreme risks with RPN more than 100, high risks with RPN more than 60 until 100, medium risks with RPN more than 20 until 60, and low risks with RPN 20 or less. Here is a chart that visualizes the level of the risks.

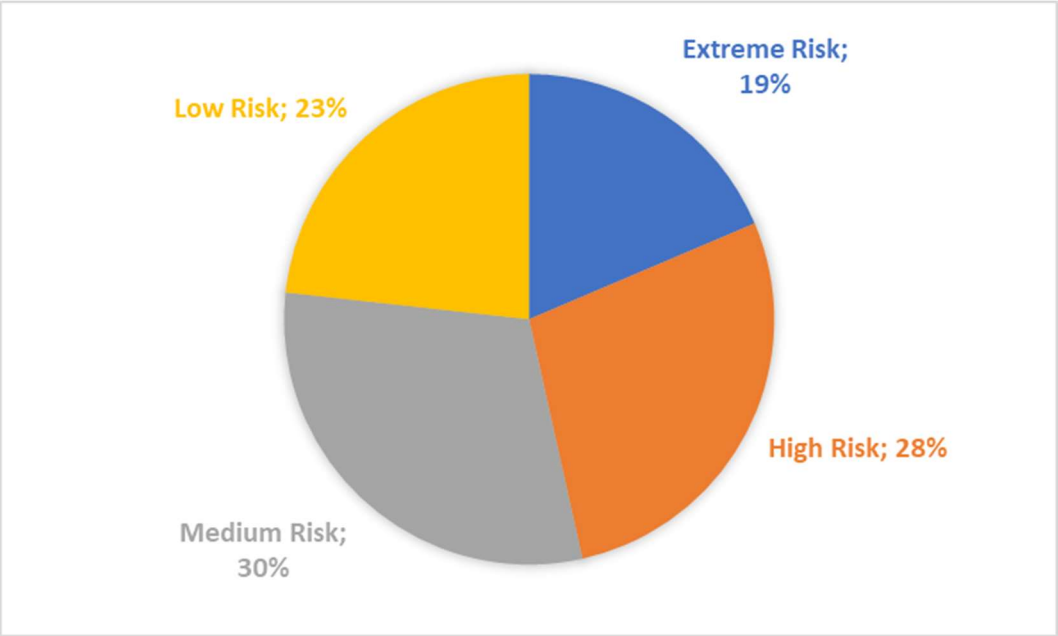

Figure 5.4 Risk Level Proportion

Next, the prioritized risks are identified by using Pareto Law. By using Pareto, 20% of the total RPN value has 80% of the total risk impact. Based on Pareto, 8 risks are being prioritized, which have RPN value of 125. Besides, risks with severity score of 5 also included as prioritized risks. In total, there are 19 risks that are being prioritized. With addition of extreme and high level of risks, there are 28 risks that must be treated. The risks that are must be treated are risks that have to be anticipated by the company because those have more significant impact, are likely to happen, and harder to be identified than the other risks.

5.3 Analysis of Operational Risk Treatment Alternative Scenario Determination

Every risk has consequences. To reduce those consequences, the company has to do treatment actions. In this part, the risks are grouped into several category based on the similarity of the risk scope, which are website, fraud report, dealing process, and service way of use. Then, the category will be broken down into several sub-category. Website category is differentiated into before using the service and while using the service. Fraud report is differentiated into form, verification, database, amount, and reliability. Dealing process is differentiated into

needs, email, appointment, demo day, and contract. Service way of use does not have any sub-category. Those sub-categories consist of several risks and can be treated by a single or more risk treatment action. That means, a risk treatment can solve more than one risk and a risk treatment action can solve several risks with more than one risk source. At least one alternative risk treatment is assigned to every risk. For the risks that have two alternative risk treatments, the treatments can be either two reduce action or a reduce action with a "do nothing" action or called accept risk. If a risk has two reduce actions as the alternative treatments, each of them will be to reduce the occurrence score and the other is to reduce the severity score. Treatments with purpose to reduce severity and to reduce occurrence have different benefit that the company will get. The reduce actions are also differentiated into preventive and curative. Preventive refers to action that can prevent the impact the risk before the risk happens. While curative refers to action that can fix the damage from the impact of the risk after the risk happens. Avoidance is not being considered because the company must spend a lot of cost to avoid a risk since the probability of the risk occurrence has to be removed completely by changing the activity that causes the risks. Thus, it is not suitable for a startup that needs to minimize the cost usage. Also, there is no risk with transfer action because there is no risk that can be solved by transferring the impact to another party.

The next part is the scenario determination. Six combinations of treatments are conducted as four different scenarios. Scenario 1 and scenario 2 are applying reduce actions as the treatment to all risks. Scenario 3 and scenario 4 are the development of scenario 1. While scenario 5 and scenario 6 are the development of scenario 2. Scenario 3 and scenario 4 are reducing medium, high, and extreme risks while accepting low risks that are included as non-prioritized risks. Scenario 4 and scenario 6 are reducing high and extreme risks while accepting low and medium risks that are included as non-prioritized risks. These scenarios are formulated to find out which combination of treatments that give the highest benefit compared to its cost.

5.4 Analysis of Operational Risk Treatment Alternative Scenario Assessment

In this part, all of the formulated scenarios are being compared each other by using benefit cost ratio. Benefit cost ratio is used to define if the risk treatments of each scenario are feasible in term of the benefit that is taken by doing those risk treatments. However, in this research, this method is done also to choose the best scenario by using incremental benefit cost ratio. Since Kredibel is a profit company, all the decisions are profit oriented. Thus, benefit cost ratio is chosen rather than other alternative selection method.

The first step of benefit cost ratio is to define the benefit component of each treatment action. Benefit component refers to profit that the company can get if the action is done. The benefit that a company can get if a risk is being treated depends on the treatment action. A treatment action that has a purpose to reduce the severity of a risk may give different benefit with a treatment action that has a purpose to reduce the occurrence of the same risk. Thus, the benefit component identification is differentiated into two, which are the treatment actions that have a purpose to reduce the severity and the other ones that have a purpose to reduce the occurrence. In total, there are 7 benefit components that are able to being identified. After that, the proxy of every benefit component is identified. The proxy is adjusted based on the current condition of the company. Proxy of the benefit component refers to the profit that is directly obtained by the company or the cost that is possibly reduced. Data and information that is required in the making and calculation of proxy are gathered by doing direct interview to the company's representative.

The next step of benefit cost ratio is to define the cost component of each treatment action. The cost that is identified is the cost that occurs only when the risk treatments are done. The cost is differentiated into two, which are Capital Expenditure (CAPEX) and Operational Expenditure (OPEX). The cost components are identified based on the treatment actions and grouped into two same as the benefit component identification, which are the treatment actions that have a purpose to reduce the severity and the other ones that have a purpose to reduce the occurrence. The severity reduction risk treatment, there are 7 CAPEX cost components and 4 OPEX cost components. While for the occurrence reduction risk

treatment, there are 2 CAPEX cost components and 9 OPEX cost components. In total, there are 9 CAPEX cost components and 13 OPEX cost components. After that, the proxy is also identified for each cost component, which is based on company's current condition. Similar with the benefit components, data and information that is required in the making and calculation of proxy are gathered by doing direct interview to the company's representative and also secondary data for the cost that never been used before by the company.

Finally, the present value of benefit and cost are calculated for each scenario. Here is the total benefit and cost value of every scenario. It can be seen in from the graph that all the scenarios are feasible because the benefit is higher than the cost or the benefit cost ratio is higher than 1.

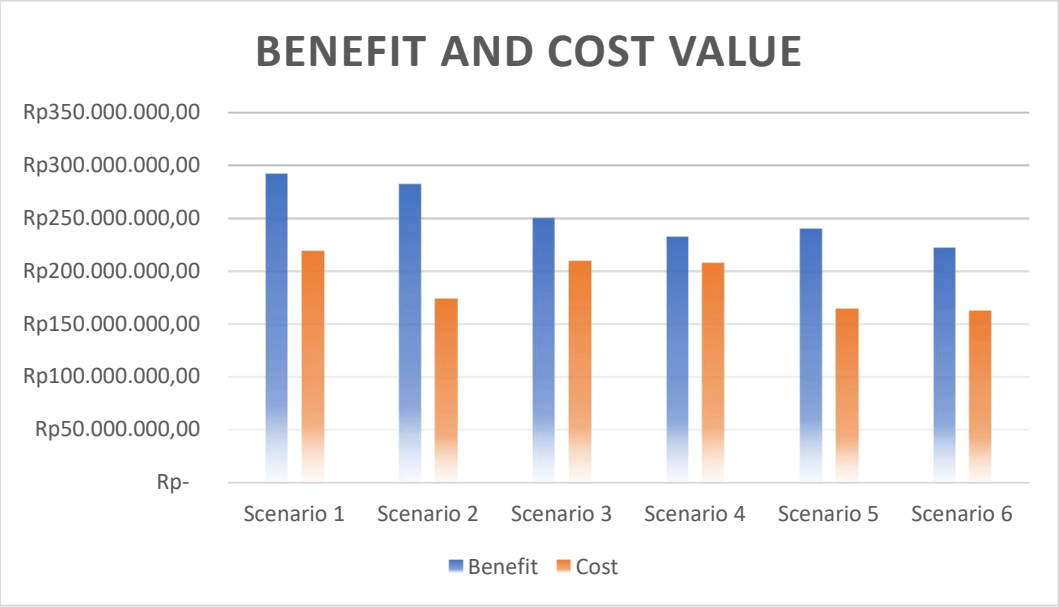

Figure 5.5 Benefit and Cost Present Value for Every Scenario

Then, the benefit cost ratio is calculated by dividing benefit value with cost value. The benefit cost ratio for all the scenarios is in a range between 1.34 until 1.62. It means, all the scenarios are feasible to be implemented. To choose which scenario to be implemented in Kredibel, incremental benefit cost ratio is conducted for all the six scenarios. Based on the incremental benefit cost ratio calculation, scenario 2 is chosen as the most preferable scenario to be implemented. Thus, it is better to apply mitigate treatments which are reduce actions to all the low, medium, high,

and extreme risks. Here are the risk treatments that are contained in the most preferable scenario which is scenario 2 along with the explanation for each risk treatment.

1. Provide call center or customer care to respond complaints from users/clients about error on the website and questions from users/clients about how to use the website, so that the problem can be fixed immediately. It is better to provide customer care using a manpower rather than a bot because manpower can solve any case includes the case that is rarely happened. Usually, company that uses bot in their customer care also place a manpower to solve special cases. The cost is too high for Kredibel to use both bot and manpower. Moreover, an intern worker is enough to be placed as the customer care instead of a full-time worker.
2. Provide an employee that responsible to be the technician for every client. By providing a person in charge for every client, the problems that are occurred can be handled immediately and the clients can use the service again as soon as possible. This position also can be filled by intern workers. An intern worker only handles one client at a time. However, it is still possible to handle more than one client per worker.
3. Allow user to edit reports after submitting them. So that, the user can fix their reports after they submitted them. The reports needed to be edited because either there is mistake in the report, the report is less detailed, or it is accidentally submitted before it is done.
4. Organize training twice a year for the workers that are responsible to verify the reports. This training is done in order to increase the effectivity of the report verification process so that the number of checked reports can be increased since the verifier is paid per hour not per report.
5. Allow user to monitor the submitted report and can resubmit the report if it is not submitted or complaint if the report is not processed after several day. This feature may educate the user to fill the report properly because they are aware if their report is already following the requirement or not. The report that is not following the requirement can be resubmitted. Thus, it can reduce the number of unverified reports.

6. Use Instagram ads to raise awareness and influence people to report their fraud experience. This action is effective because Instagram is one of social media applications that has a specific online shop feature. Thus, there is possibility of fraud in Instagram and Instagram users are included as active online shopper.
7. Allow user to give like or dislike for each report as additional reference. Likes toward a report are counted separately with how many it is being reported. This action is done to prevent fake reports toward a trusted store and a fraud store. The likes also can be used as additional consideration of the validity of a report.
8. Allow user to monitor the submitted needs and can edit them if it is not following the requirements. It may facilitate the clients to explain their needs properly in the shortest possible time.
9. Provide adequate performance management to prevent workers to make mistakes in sending email. It is a software based that is provided by a third party. It is done to prevent any mistakes in order to maintain the customer satisfaction.
10. Send a follow-up email if the client does not respond in two days after the confirmation email sent. This action is done in case the previous email is not arrived at the client or the response email to the previous email is not arrived at Kredibel. This action may increase the number of clients.
11. Add reminder on the website for client to always check their spam folder. It is done to reduce the dealing process duration and it may increase the number of clients that uses service that is provided by Kredibel.
12. Add multiple input form of proposed appointment date while requesting the service. This action can increase the efficiency of the appointment process. The clients may give several options of meeting date and Kredibel can choose a day that match with their schedule easily.
13. Organize a regular evaluation twice a year for the service description, includes what can be fulfilled, how the service run, and the basic terms and condition based on the client's feedback. This action is done to make sure that the clients are fully understood about the service.

14. Organize a regular evaluation four times a year related to the SOP of non-disclosure agreement between Kredibel and the client. This action is done to minimize the possible mistakes regarding the making of NDA, which are mistakes that occurs because of human error, terms and condition that accidentally bring harm to Kredibel, or some factors that is not considered yet during the NDA formulation.
15. Conduct different SOP related to service fulfillment for each client. Since every client has different requirements, separated SOP is needed to make sure that all client's requirements are fulfilled properly. It may maintain the customer satisfaction and prevent the company to pay any fine.
16. Provide an employee for clients that responsible to make sure that the client is able to use the service (customer support). Besides customer care that focus on accommodating any complaints from the users and prospective clients, customer support also needed to accommodate the clients that directly use the service. This position also can be filled by intern worker.

(This page is intentionally left blank)

CHAPTER 6
CONCLUSION AND SUGGESTION

In this chapter, there will be conclusion regarding this research based on the objectives that already determined by the author in the beginning of this research and also suggestion from the author to improve the further research development.

6.1 Conclusion

Based on the data processing, analysis, and interpretation of this research, here are several conclusions that can be taken.

1. Potential failures or risks identification in operational activities of PT Kredibel Teknologi Indonesia is done using Failure Mode and Effect Analysis (FMEA) and based on service blueprint that is already conducted previously. Based on the risk identification to 24 activities from 3 processes, there are 43 operational risks found with different cause, impact, and control.
2. Risk profile determination is done based three dimensions, which are severity, occurrence, and detection. Score of every dimension is in a range of 1 to 5. Each score has its own indicator that is validated by the company. Risk Priority Number (RPN) is used to define each risk level and risks that are included as prioritized risks. The RPN is calculated by multiplying severity score with occurrence score and detection score of each risk. Then, the RPN of the risks are categorized into low risk, medium risk, high risk, and extreme risks. There are 23% of low risks, 30% of medium risks, 28% of high risks, and 19% of extreme risks. The RPN also used to determine the prioritized risks using Pareto. Also, risks that have severity score of 5 are also included as prioritized risks. Since extreme and high risks are included as risks that must be treated, in total there are 28 risks that must be treated.
3. Alternatives of risk treatment are assigned to every risk. A risk can have one or maximum two alternatives. The risk treatments are either reduce risk or accept risk because there is no risk that can be avoided or

transferred. These risk treatment alternatives are formulated into six different scenarios. Scenario 1 and scenario 2 are reducing all risks, scenario 3 and scenario 5 are reducing all prioritized risks and medium risks, and scenario 4 and scenario 6 are only reducing prioritized risks.

4. Benefit cost ratio is conducted to choose the best risk treatment alternative scenario by considering the benefit and cost that might happened if the treatments are done during 2021 and 2022. There are 7 benefit components and 22 cost components, which are 9 CAPEX components and 13 OPEX components that are being identified. The present value of the benefit is ranged between Rp222.000.000 until Rp292.020.202. While for the cost is ranged between Rp162,555,228 until Rp218,649,773. The result of benefit cost ratio calculation is 1.34 for scenario 1, 1.62 for scenario 2, 1.20 for scenario 3, 1.12 for scenario 4, 1.46 for scenario 5, and 1.37 for scenario 6. Thus, all the scenarios are feasible to be implemented and the most preferable risk treatments to be implemented based on the incremental benefit cost ratio are the ones that are included in scenario 2.

6.2 Suggestion

Here are some suggestions that can be used in the improvement and development of further similar research.

1. Fault Tree Analysis (FTA) method may be used to define the relationship between multiple failures to improve the risk identification.
2. It is necessary to evaluate the risk treatments after being implemented and calculate the resulting RPN of each risk.
3. Strategic activities may be involved to identify the strategic risks of the company.
4. Considering non-financial benefit that is not directly obtained by the company can complete the research.
5. The risk assessment is done based on current internal and external condition of the company, so it is necessary to do risk assessment regularly. Once the company's condition being changed, there are several things that may

change, which are number or risk, RPN calculation, risk rank, and mitigation plan.

(This page is intentionally left blank)

REFERENCE

Action Fraud, t.thn. *Online Shopping Fraud.* [Online] Available at: https://www.actionfraud.police.uk/a-z-of-fraud/online-shopping-fraud
[Accessed 27 January 2021].

ASQ, 2021. *FAILURE MODE AND EFFECTS ANALYSIS (FMEA).* [Online] Available at: https://asq.org/quality-resources/fmea
[Accessed 26 January 2021].

Association for Project Management, 2020. *Risk Management.* [Online] Available at: https://www.apm.org.uk/resources/what-is-project-management/what-is-risk-management/
[Accessed 2 February 2021].

Blackman, A., 2014. *The Main Types of Business Risk.* [Online] Available at: https://business.tutsplus.com/tutorials/the-main-types-of-business-risk--cms-22693
[Accessed 2 February 2021].

Carlson, C., 2018. *Understanding FMEA Occurrence Risk – Part 1.* [Online] Available at: https://accendoreliability.com/understanding-fmea-occurrence-risk-part-1/
[Accessed 4 February 2021].

Carlson, C., 2018. *Understanding FMEA Severity Risk – Part 1.* [Online] Available at: https://accendoreliability.com/understanding-fmea-severity-part-1/
[Accessed 4 February 2021].

Carlson, C., 2019. *Understanding FMEA Detection: Part 1.* [Online] Available at: https://accendoreliability.com/understanding-fmea-detection-part-1/
[Accessed 4 February 2021].

CIO Wiki, 2020. *Risk Management.* [Online] Available at: https://cio-

wiki.org/wiki/Risk_Management#Benefits_of_Risk_Management
[Accessed 3 February 2021].

Cole, B., 2020. *Risk Management.* [Online] Available at: https://searchcompliance.techtarget.com/definition/risk-management
[Accessed 3 February 2021].

Confirmative, 2021. *SIMILARITIES BETWEEN ISO 9001, ISO 14001 AND ISO 31000.* [Online] Available at: http://www.confirmative.com.au/2017/04/iso9001-iso14001-iso31000.html
[Accessed 26 January 2020].

Corporate Finance Institute, 2015. *Business Risk.* [Online] Available at: https://corporatefinanceinstitute.com/resources/knowledge/finance/business-risk/
[Accessed 2 February 2021].

Corporate Finance Institute, 2015. *Risk Management.* [Online] Available at: https://corporatefinanceinstitute.com/resources/knowledge/strategy/risk-management/
[Accessed 3 February 2021].

Creately, 2020. *The Easy Guide to Creating an Effective Service Blueprint.* [Online] Available at: https://creately.com/blog/diagrams/what-is-a-service-blueprint/
[Accessed 17 February 2021].

DSI International, 2017. *How to Avoid Failures-(FMEA and/or FTA).* [Online] Available at: https://www.dsiintl.com/wp-content/uploads/2017/04/HOW-TO-AVOID-FAILURES-FMEA-andor-FTA.pdf
[Accessed 4 February 2021].

EduPristine, 2018. *All you want to know about Sensitivity Analysis.* [Online] Available at: https://www.edupristine.com/blog/all-about-sensitivity-

analysis
[Accessed 4 February 2021].

Enterprise Risk Management Academy, 2010. *ISO 31000 Risk Management Standard.* [Online] Available at: https://erm-academy.org/risk-management-knowledge/iso-31000-risk-management-standard
[Accessed 3 February 2021].

Gibbons, S., 2017. *Service Blueprints: Definition.* [Online] Available at: https://www.nngroup.com/articles/service-blueprints-definition/
[Accessed 17 February 2021].

Hariri, R. H., Fredericks, E. M. & Bowers, K. M., 2019. Uncertainty in big data analytics: survey, opportunities, and challenges. *Journal of Big Data,* 6(44).

Infraspeak, t.thn. *FTA vs FMEA: What Are The Differences?*. [Online] Available at: https://blog.infraspeak.com/fta-vs-fmea/
[Accessed 2 February 2021].

Intaver Institute, t.thn. *Calculating Risk Scores.* [Online] Available at: http://intaver.com/risk-scores/#:~:text=Risk%20score%20is%20a%20calculated,also%20be%20part%20of%20calculation.
[Accessed 2 March 2021].

Integrate Definition Methods, 2021. *IDEFØ Function Modeling Method.* [Online] Available at: https://www.idef.com/idefo-function_modeling_method/
[Accessed 4 February 2021].

ISO, 2018. *ISO 31000;2018.* [Online] Available at: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
[Accessed 3 February 2021].

JawaPos.com, 2019. *Pemakaian Big Data di Indonesia Meningkat.* [Online] Available at: https://www.jawapos.com/ekonomi/bisnis/21/11/2019/pemakaian-big-data-di-indonesia-meningkat/
[Accessed 26 January 2021].

Kenton, W., 2020. *Business Continuity Planning (BCP).* [Online] Available at: https://www.investopedia.com/terms/b/business-continuity-planning.asp
[Accessed 17 February 2021].

Kenton, W., 2020. *Cost-Benefit Analysis.* [Online] Available at: https://www.investopedia.com/terms/c/cost-benefitanalysis.asp
[Accessed 4 February 2021].

Kenton, W., 2020. *Sensitivity Analysis.* [Online] Available at: https://www.investopedia.com/terms/s/sensitivityanalysis.asp
[Accessed 4 February 2021].

Kosutic, D., 2014. *ISO 31000 and ISO 27001 – How are they related?.* [Online] Available at: https://advisera.com/27001academy/blog/2014/03/31/iso-31000-and-iso-27001-how-are-they-related/
[Accessed 2 February 2021].

Kredibel, 2016. *About Us.* [Online] Available at: https://kredibel.co.id/about?__cf_chl_jschl_tk__=f38dc4ea1cfd3c81314239cbf3f0d8c57a2f5df8-1611644371-0-AWdGbapg_YS33OXpZpIjcy8FSDPv8mcFP5fz9lJtmYcnAtpQrdWGAuOsdZYXD3-LPjdQc1ASw3CQ8bOfq_xbvAbfAUa9ypErpqeTB9SvhRwc4QGp59J1yjW7BzPqN1o6gcZzRfcRwNySLj2g7Og-XvzW
[Accessed 26 January 2021].

Lewis & Clark, 2010. *What is "online fraud"?.* [Online] Available at: https://law.lclark.edu/live/news/6855-what-is-online-fraud#:~:text=Fraud%20that%20is%20committed%20using,financial%20fraud%20and%20identity%20theft.&text=Often%20financial%20fraud%20can%20lead,the%20victim%27s%20bank%20account%20information.
[Accessed 27 January 2021].

Long, R., 2017. *What is Business Continuity? – Business Continuity 101.* [Online] Available at: https://www.mha-it.com/2017/08/01/what-is-business-

continuity/
[Accessed 18 February 2021].

Mallens, E. & Kruf, J. P., 2013. *ISO 31000.* [Online] Available at: https://primo-europe.eu/iso-31000/ [Accessed 3 February 2021].

Niedbala, C., 2020. *Risk Management: Avoid, Reduce, Transfer or Accept?*. [Online] Available at: https://foundershield.com/risk-management/ [Accessed 4 February 2021].

Novianty, D., 2020. *Adopsi Big Data dan AI di Indonesia Semakin Luas.* [Online] Available at: https://www.suara.com/tekno/2020/11/30/101611/adopsi-big-data-dan-ai-di-indonesia-semakin-luas [Accessed 26 January 2021].

Pereira, 2019. *10 Steps to Creating a FMEA.* [Online] Available at: https://blog.gembaacademy.com/2007/06/28/10-steps-to-creating-a-fmea/ [Accessed 18 February 2021].

Peterson, O., 2019. *What Is ISO 31000? Getting Started with Risk Management.* [Online] Available at: https://www.process.st/iso-31000/#what_is_iso_31000 [Accessed 26 January 2021].

Praxiom, 2018. *ISO 31000 2018.* [Online] Available at: https://www.praxiom.com/iso-31000-terms.htm#Risk [Accessed 2 February 2021].

Pugh, M.-R., 2021. *What Is a Service Blueprint?: Designing a Seamless Service Process.* [Online] Available at: https://www.lucidchart.com/blog/what-is-a-service-blueprint [Accessed 17 February 2021].

Quality Training Portal, 2021. *10 Steps to Conduct a PFMEA.* [Online] Available at: https://qualitytrainingportal.com/resources/fmea-resource-center/traditional-rpn-fmea/10-steps-conduct-pfmea/ [Accessed 4 February 2021].

Risk Decisions, 2020. *4 Great reasons to adopt the ISO 31000 risk management standard.* [Online]
Available at: https://www.riskdecisions.com/four-great-reasons-to-adopt-the-iso-31000-risk-management-standard/
[Accessed 26 January 2021].

Rouse, M., 2020. *Risk Management.* [Online]
Available at: https://searchcompliance.techtarget.com/definition/risk-management#:~:text=Risk%20management%20is%20the%20process,errors%2C%20accidents%20and%20natural%20disasters.
[Accessed 26 January 2021].

SAS, 2021. *Big Data Analytics What it is and why it matters.* [Online]
Available at: https://www.sas.com/en_us/insights/analytics/big-data-analytics.html
[Accessed 26 January 2021].

Schenkelberg, F., 2014. *10 Steps of FMEA.* [Online]
Available at: https://accendoreliability.com/10-steps-of-fmea/
[Accessed 4 February 2021].

Schroer, A., 2019. *34 BIG DATA COMPANIES HELPING US MAKE SENSE OF THE WORLD.* [Online]
Available at: https://builtin.com/big-data/big-data-companies-roundup
[Accessed 26 January 2021].

Sebastian, 2021. *What Is the Benefit Cost Ratio (BCR)? Definition, Formula, Example.* [Online]
Available at: https://project-management.info/benefit-cost-ratio/
[Accessed 4 February 2020].

Security Magazine, 2017. *E-Commerce Fraud Loss Reaches $57.8 Billion.* [Online]
Available at: https://www.securitymagazine.com/articles/88451-e-commerce-fraud-loss-reaches-578-billion
[Accessed 27 January 2021].

Service Design Tools, t.thn. *Service Blueprint.* [Online]
Available at: https://servicedesigntools.org/tools/service-blueprint
[Accessed 17 February 2021].

Sullivan, E., 2020. *What is business continuity and why is it important?*. [Online] Available at: https://searchdisasterrecovery.techtarget.com/definition/business-continuity
[Accessed 18 February 2021].

Syque, t.thn. *ICOM.* [Online] Available at: http://www.syque.com/improvement/ICOM.htm
[Accessed 4 February 2021].

Technopedia, 2021. *Integration Definition (IDEF).* [Online] Available at: https://www.techopedia.com/definition/19924/integration-definition--idef
[Accessed 4 February 2021].

The Economic Times, 2020. *Definition of 'Cost Benefit Analysis'.* [Online] Available at: https://economictimes.indiatimes.com/definition/cost-benefit-analysis
[Accessed 4 February 2021].

The New Daily, 2019. *Australians have lost more than $4 million to online shopping scams in 2019.* [Online] Available at: https://thenewdaily.com.au/finance/consumer/2019/11/25/online-shopping-scams-2019/
[Accessed 27 January 2021].

The Strategic CFO, 2020. *Sensitivity Analysis Definition.* [Online] Available at: https://strategiccfo.com/sensitivity-analysis-definition/
[Accessed 4 February 2021].

Veyrat, P., 2016. *What is the definition of risk management?*. [Online] Available at: https://www.heflo.com/blog/risk-management/what-is-the-definition-of-risk-management/
[Accessed 3 February 2021].

Wilson, M., 2020. *Risk Management – Definition, Strategies and Processes.* [Online]

Available at: https://www.pcwdld.com/definition/risk-management [Accessed 26 January 2021].

Yeo, S., 2019. *https://thenewdaily.com.au/finance/consumer/2019/11/25/online-shopping-scams-2019/.* [Online] Available at: https://www.techinasia.com/examining-online-fraud-southeast-asia [Accessed 27 January 2021].

ATTACHMENT 1
RISK VALIDATION QUESTIONNAIRE

Validator

Name :

Position :

RISK VALIDATION SHEET

Feeling Instruction:

1. Please put a “V” in column “Valid” if the risk is possible to happen or in column “Not Valid” if the risk is not possible to happen.
2. If the risk is not valid, please specify the reason or revision in column “Notes”.
3. If the risk is valid, please put a "V" in column "Ever Happened" if the risk ever happened before or in column "Never Happened" if the risk never happen before.
4. If there are risks that are not listed yet, please write it down in “Additional Risk” table below the risk table by write it down along with the Activity Code.

The table below consists of risks that are possibly happen in the service offered by PT. Kredibel Teknologi Indonesia. The risks are identified based on the determined activities and differentiated into three sources, which are user/client, system, and employee.

Activity Code	Activity	Risk Source	Risk	Validation		If Valid		Notes (If Not Valid)
				Valid	Not Valid	Ever Happened	Never Happen	
A-1.1	Visit website	System	The website cannot be accessed by user					
A-2.1	Welcome to website	User/Client	The user finds it hard to find "Laporkan Penipuan" button					
A-1.2	Visit “Laporkan Penipuan” page	User/Client	The user makes mistake in filling out the report form					
			The user deliberately submitted a fake report					

Activity Code	Activity	Risk Source	Risk	Validation		If Valid		Notes (If Not Valid)
				Valid	Not Valid	Ever Happened	Never Happen	
			The report submitted is less detailed					
			The report is not included as a fraud case					
		System	"Laporkan Penipuan" page cannot be accessed by user					
A-2.2	Welcome to “Laporkan Penipuan” page	User/Client	The user does not understand how to fill the form					
A-1.3	Submit fraud information	User/Client	The report accidentally					

Activity Code	Activity	Risk Source	Risk	Validation		If Valid		Notes (If Not Valid)
				Valid	Not Valid	Ever Happened	Never Happen	
			submitted when it is not finished yet					
		System	The report cannot be submitted					
			The report is submitted but not recorded in the database					
A-3.1	Verify fraud information	Employee	The fake/wrong report is verified					
			The real/good report is not verified					

Activity Code	Activity	Risk Source	Risk	Validation		If Valid		Notes (If Not Valid)
				Valid	Not Valid	Ever Happened	Never Happen	
B-1.1	Visit website	System	The website cannot be accessed by client					
B-2.2.1	Welcome to website	User/Client	The client finds it hard to find "Enterprise" button					
B-1.2	Visit page for enterprise	System	The client failed to login					
B-2.2.2	Welcome to page for enterprise	User/Client	The client does not understand the description of the service					

Activity Code	Activity	Risk Source	Risk	Validation		If Valid		Notes (If Not Valid)
				Valid	Not Valid	Ever Happened	Never Happen	
B-1.3	Request a demo based on needs	User/Client	The submitted needs are less detailed					
			The submitted needs is not clear					
B-2.1.3	Request demo day schedule	Employee	The proposed date is not approved by the client					
B-1.4	Approve demo day schedule	Employee	The email is forgotten to be sent					
			There is a mistake in email					

Activity Code	Activity	Risk Source	Risk	Validation		If Valid		Notes (If Not Valid)
				Valid	Not Valid	Ever Happened	Never Happen	
		System	The email is sent but not arrive to the client					
			The email goes to spam folder					
B-1.5	Set the requirement	Employee	The proposed requirement from the client cannot be fulfilled by Kredibel					
			There is a misperception toward the needs					
B-2.1.2	Make contract	User/Client	The client does not understand					

Activity Code	Activity	Risk Source	Risk	Validation		If Valid		Notes (If Not Valid)
				Valid	Not Valid	Ever Happened	Never Happen	
			how the service run					
		Employee	There is mistake inside the contract					
			Kredibel is failed to fulfill the agreed requirement					
B-3.1	Prepare terms & condition and set the price	Employee	The terms & condition are not approved by the client					
			The terms & condition bring					

Activity Code	Activity	Risk Source	Risk	Validation		If Valid		Notes (If Not Valid)
				Valid	Not Valid	Ever Happened	Never Happen	
			harm to Kredibel					
			There are some factors that is forgetten to consider					
B-2.1.3	Send API key to the client	Employee	The API key is given late					
C-1.1	Insert API key	User/Client	The client does not understand how to insert API Key					
		System	API Key cannot be used					

Activity Code	Activity	Risk Source	Risk	Validation		If Valid		Notes (If Not Valid)
				Valid	Not Valid	Ever Happened	Never Happen	
C-2.1	Confirm API key	System	The API Key confirmation is not sent					
C-1.2	Refill billing	User/Client	The client does not understand how to refill billing					
		System	Billing cannot be used					
C-2.2	Confirm billing	System	The billing confirmation is not sent					
C-1.3	Insert query	User/Client	The client makes mistake in inserting query					

Activity Code	Activity	Risk Source	Risk	Validation		If Valid		Notes (If Not Valid)
				Valid	Not Valid	Ever Happened	Never Happen	
C-2.3	Screening	User/Client	The client does not understand the screening report					
		Employee	There is error in screening report					
C-3.1	Provide database	System	There is no sufficient data/the data is less accurate					
			The real/non-fraudster account classified as fake/fraudster account					

Activity Code	Activity	Risk Source	Risk	Validation		If Valid		Notes (If Not Valid)
				Valid	Not Valid	Ever Happened	Never Happen	
			The fake/fraudster account classified as real/non-fraudster account					

Additional Risks:

Activity Code	Risk	Notes

……, …… 2021

Position

(*Name*)

(This page is intentionally left blank)

ATTACHMENT 2

RISK SCORE RATING VALIDATION QUESTIONNAIRE

Validator

Name :

Position :

RISK SCORE RATING VALIDATION SHEET

Feeling Instruction:

1. Please put a "V" in column "Valid" if the rating is suitable to the company's preference or in column "Not Valid" if the rating is not suitable to the company's preference.
2. If the rating is not valid, please specify the reason and/or revision in column "Notes".

The table below consists of risk score rating for every aspect, which are severity, occurrence, and detection. These aspects will be used to define the level of each risk.

Aspect	Category	Description	Rating	Validation		Notes (If Not Valid)
				Valid	Not Valid	
Severity	Extreme	Risk can cause major disruption to service fulfillment (all service fulfillment stops)	5			

Aspect	Category	Description	Rating	Validation		Notes (If Not Valid)
				Valid	Not Valid	
	Heavy	Risk can cause major disruption to service fulfillment (give impact on most of the service fulfillment processes, the service provided do not meet quality standards and require repetition of several aspects of the service).	4			
	Medium	Risk can cause moderate disruption to service fulfillment (give impact on several	3			

Aspect	Category	Description	Rating	Validation		Notes (If Not Valid)
				Valid	Not Valid	
		service fulfillment processes, and the service provided do not meet quality standards)				
	Light	Risk can cause moderate disruption to service fulfillment (give impact on related process, the service provided is slightly below quality standards but can be fixed)	2			
	Insignificant	Risk may cause minor	1			

Aspect	Category	Description	Rating	Validation		Notes (If Not Valid)
				Valid	Not Valid	
		interruptions that do not have a significant impact on service quality				
Occurrence	Almost certain	Cause of risk can occur (based on experience for the past 3 months)	5			
	May occurred	Cause of risk can occur (based on experience from 3 months to 1 year ago)	4			
	Not common but can be occurred	Cause of risk can occur (based on experience from 1 year	3			

Aspect	Category	Description	Rating	Validation		Notes (If Not Valid)
				Valid	Not Valid	
		to 2 years ago)				
	Unlikely	Cause of risk can occur (based on experience from 2 years to 3 years ago)	2			
	Much less likely	Cause of risk never occurs (based on experience for the past 3 years)	1			
Detection	Almost impossible	The checking system has no possibility of detecting risk	5			
	High	The checking system has a low chance	4			

Aspect	Category	Description	Rating	Validation		Notes (If Not Valid)
				Valid	Not Valid	
		of detecting risk				
	Moderate	The checking system has a moderate chance of detecting risk	3			
	Low	The checking system has a high chance of detecting risk	2			
	Almost certain	The checking systems can almost certainly detect risk	1			

……, …… 2021

Position

(*Name*)

ATTACHMENT 3

RISK SCORE ASSESSMENT QUESTIONNAIRE

Validator

Name :

Position :

RISK SCORE RATING INDICATOR

Severity		
Category	**Description**	**Rating**
Extreme	Risk can cause major disruption to service fulfillment (**all service fulfillment stops**)	**5**
Heavy	Risk can cause major disruption to service fulfillment (give impact on **most of the service fulfillment processes**, the service provided **do not meet quality standards** and **require repetition** of several aspects of the service)	**4**
Medium	Risk can cause moderate disruption to service fulfillment (give impact on **several service fulfillment processes,** and the service provided **do not meet quality standards**)	**3**
Light	Risk can cause moderate disruption to service fulfillment (give impact on **related process**, the service provided is **slightly below quality standards** but can be fixed)	**2**
Insignificant	Risk may cause minor disruptions that **do not have a significant impact on service quality**	**1**

Occurrence		
Category	**Description**	**Rating**
Almost certain	Cause of risk can occur (based on experience for the **past 3 months**)	**5**

Occurrence		
Category	**Description**	**Rating**
May occurred	Cause of risk can occur (based on experience from **3 months to 1 year ago**)	**4**
Not common but can be occurred	Cause of risk can occur (based on experience from **1 year to 2 years ago**)	**3**
Unlikely	Cause of risk can occur (based on experience from **2 years to 3 years ago**)	**2**
Much less likely	Cause of risk never occurs (based on experience for the **past 3 years**)	**1**

Detection		
Category	**Description**	**Rating**
Almost impossible	The checking system has **no possibility** of detecting risk	**5**
High	The checking system has a **low** chance of detecting risk	**4**
Moderate	The checking system has a **moderate** chance of detecting risk	**3**
Low	The checking system has a **high** chance of detecting risk	**2**
Almost certain	The checking systems can **almost certainly** detect risk	**1**

RISK SCORE ASSESSMENT SHEET

Feeling Instruction:

Please fill severity score, occurrence score, and detection score in a range of 1 to 5. The description of each rating can be seen in the risk score rating table.

The table below consists of risk impact, cause, and control that can be used as additional consideration for defining severity, occurrence, and detection score rating. These scores will be used to define the level of each risk.

Risk Code	Risk	Risk Impact	Severity Score	Risk Cause	Occurrence Score	Risk Control	Detection Score
R1	The website cannot be accessed by user	Reduce user experience		Lack of website treatment procedure		None	
R2	The user finds it hard to find "Laporkan Penipuan" button	Reduce user experience		Bad UI/UX		UI/UX evaluation	
R3	The user makes mistake in filling out the report form	Reduce number of valid reports		The form instruction is less informative		None	
R4	The report submitted is less detailed	Reduce number of valid reports		The form instruction is less informative		None	

Risk Code	Risk	Risk Impact	Severity Score	Risk Cause	Occurrence Score	Risk Control	Detection Score
R5	"Laporkan Penipuan" page cannot be accessed by user	Reduce user experience		Lack of website treatment procedure		None	
R6	The user does not understand how to fill the form	Reduce number of valid reports		The form instruction is less informative		None	
R7	The report accidentally submitted when it is not finished yet	Reduce number of valid reports		Bad UI/UX		None	
R8	The report cannot be submitted	User cancels submit the report		Lack of website treatment procedure		Website checking	

Risk Code	Risk	Risk Impact	Severity Score	Risk Cause	Occurrence Score	Risk Control	Detection Score
R9	The report is submitted but not recorded in the database	Reduce number of valid reports		Lack of website treatment procedure		None	
R10	The fake/wrong report is verified	Reduce data reliability		Lack of report standarization		None	
R11	The real/good report is not verified	Reduce data reliability		Lack of report standarization		None	
R12	The website cannot be accessed by client	Reduce customer experience of client		Lack of website treatment procedure		None	
R13	The client finds it hard to find "Enterprise" button	Reduce customer experience of client		Bad UI/UX		UI/UX evaluation	

Risk Code	Risk	Risk Impact	Severity Score	Risk Cause	Occurrence Score	Risk Control	Detection Score
R14	The client failed to login	Reduce number of client		Lack of website treatment procedure		None	
R15	The client does not understand the description of the service	Reduce number of client		The website is less informative		None	
R16	The submitted needs are less detailed	The service is not matched with the client		The needs instruction is less informative		None	
R17	The submitted needs is not clear	Lengthen the agreement process		The needs instruction is less informative		None	

Risk Code	Risk	Risk Impact	Severity Score	Risk Cause	Occurrence Score	Risk Control	Detection Score
R18	The proposed date is not approved by the client	Lengthen the agreement process		Lack of date determination procedure		None	
R19	The email is forgotten to be sent	Client cancels using the service		Lack of service operation procedure		Approval email checking	
R20	There is a mistake in email	Client cancels using the service		Lack of email making procedure		Approval email checking	
R21	The email is sent but not arrive to the client	Client cancels using the service		Lack of approval email monitoring		None	
R22	The email goes to spam folder	Client cancels		Lack of approval email monitoring		None	

Risk Code	Risk	Risk Impact	Severity Score	Risk Cause	Occurrence Score	Risk Control	Detection Score
		using the service					
R23	The proposed requirement from the client cannot be fulfilled by Kredibel	Client cancels using the service		Lack of the needs standarization		None	
R24	There is a misperception toward the needs	The service is not matched with the client		Lack of the needs standarization		Historical agreement evaluation	
R25	The client does not understand how the service run	Client cancels using the service		Bad service description		Client feedback	

Risk Code	Risk	Risk Impact	Severity Score	Risk Cause	Occurrence Score	Risk Control	Detection Score
R26	There is mistake inside the contract	Delay the service usage		Lack of service operation procedure		Contract controlling before it is given to the client	
R27	Kredibel is failed to fulfill the agreed requirement	Client stops using the service		Lack of service operation procedure		Status of service monitoring	
R28	The terms & condition are not approved by the client	Lengthen the agreement process		Lack of terms & condition making procedure		None	
R29	The terms & condition bring harm to Kredibel	Higher cost		Lack of terms & condition making procedure		Compare with historical agreement	

Risk Code	Risk	Risk Impact	Severity Score	Risk Cause	Occurrence Score	Risk Control	Detection Score
R30	There is some factors that is forgetten to consider	Lengthen the agreement process		Lack of terms & condition making procedure		Compare with historical agreement	
R31	The API key is given late	Delay the service usage		Lack of employee training		Employee monitoring	
R32	The client does not understand how to insert API Key	The service cannot be used		Bad service usage instruction		None	
R33	API Key cannot be used	The service cannot be used		Lack of API Key treatment procedure		API Key monitoring	
R34	The API Key confirmation is not sent	Reduce customer satisfaction of client		Lack of service operation procedure		None	

Risk Code	Risk	Risk Impact	Severity Score	Risk Cause	Occurrence Score	Risk Control	Detection Score
R35	The client does not understand how to refill billing	The service cannot be used		Bad service usage instruction		Client feedback	
R36	Billing cannot be used	The service cannot be used		Lack of billing treatment procedure		None	
R37	The billing confirmation is not sent	Reduce customer satisfaction of client		Lack of service operation procedure		None	
R38	The client makes mistake in inserting query	The service cannot be used		The service usage instruction is less informative		Client feedback	
R39	The client does not understand the screening report	Reduce customer		The screening report is hard to understand		Client feedback	

Risk Code	Risk	Risk Impact	Severity Score	Risk Cause	Occurrence Score	Risk Control	Detection Score
		satisfaction of client					
R40	There is error in screening report	The service cannot be used		Lack of dashboard treatment procedure		None	
R41	There is no sufficient data/the data is less accurate	Client stops using the service		Lack of data		None	
R42	The real/non-fraudster account classified as fake/fraudster account	Client stops using the service		Bad data screening procedure		None	
R43	The fake/fraudster account classified as real/non-fraudster account	Client stops using the service		Bad data screening procedure		None	

Known by, ……, …… 2021

Director *Position*

(*Name*) (*Name*)

(This page is intentionally left blank)

AUTHOR BIOGRAPHY

Author, named Annura Ratri Ramadanti, was born in Jakarta, 7th of January 1999. Author is the last child of two siblings. Author formal education background started from SD Negeri Semplak 2, SMP Negeri 1 Bogor, and SMA Negeri 1 Bogor, up to this point, where the author able to finish author's Undergraduate (S1) Degree in Department of Industrial System and Engineering of Institut Teknologi Sepuluh Nopember (ITS). During author's study in Department of Industrial System and Engineering of ITS, author has contributed to several organization, committee, and project activities. Authors has contributed as the secretary and treasurer of an IE Fair event called Industrial Challenge 2019 under HMTI ITS 2018/2019, sponsorship staff of ITS EXPO 2019, fund rising supervisor of Ini Lho ITS! 2019, and Laboratory Assistant of Laboratorium Perancangan Sistem dan Manajemen Industri (PSMI) ITS from 2019 until 2021. As a laboratory assistant of PSMI Laboratory, author had the opportunity to implement knowledge and skills within the scope of PSMI Laboratory, such as assisting lecturer in conducting certain courses, tasks, tutorials, also involved in certain project related work with external parties, which are Kementerian Perindustrian and PT Star Energy Geothermal. Author got 1st place in Business Plan Competition that was held by Economic and Business Faculty, Universitas Airlangga in 2019. During the competition, author developed a healthy lifestyle application called Nutriva with her team. In 2020, author did an internship program in PT Telkom Indonesia which in Customer Directorate, Business Solution Division for 1 month. Author can be reached via email at annura.ratri@gmail.com.